Applications to Improve Privacy on Online Social Networks

Víctor Rodríguez
Universitat Politècnica de Catalunya
victorr@ac.upc.edu

Anna Carreras
Universitat Politècnica de Catalunya
annac@ac.upc.edu

Eva Rodríguez
Universitat Politècnica de Catalunya
evar@ac.upc.edu

Jaime Delgado
Universitat Politècnica de Catalunya
jaime@ac.upc.edu

ABSTRACT

Privacy management is different across the many online social networks and not always satisfies the user expectations. Some social networks members may demand choosing their privacy preferences more richly and exercise a tighter control on the information they drop. For this regard, it is under question if some of the Digital Rights Management systems features may be incorporated to the privacy management in social networks, and if the privacy terms themselves can be expressed in standardized policy languages, like XACML, additionaly bringing interoperability across the networks.

General Terms

Management, Languages, Legal Aspects

Keywords

Privacy, social networks, information sharing.

1. INTRODUCTION

Online social networks are communities in the Internet, usually around one website, which connect users voluntarily sharing information. Information exchanged through online social networks cover a broad range of topics, ranging from simple personal information to the most bizarre contents.

In the last few years, social networks have been actually *the* Internet phenomenon, and the main axis of the so called Web 2.0. According to the web traffic ranking provided by Alexa, online social networks are among the most visited web pages in the Internet. For example, Facebook, MySpace, Hi5, Twitter or Orkut are in the 50 top pages in visits. Other topic-oriented social networks take good positions in the ranking too: LinkedIn, focused on professional profiles achieves a 96th in the ranking, Flickr for the photographs exchange, a 30th position and some dating and adult sites are also in this range; sharing essentially the features with generic-oriented networks.

These Internet sites are administered by *social network providers* who usually make (or try to make) profit of the network, even though users provide information for free. The income sources of social networks providers include advertisement in the web page, data mining, use data analysis and ultimately exploitation of the contents themselves –the latter business model having been questioned.

Online social networks replicate to some extent the social relationships established in the ordinary life, with some particularities. The potential of computing and the spread of computer networks are not readily present to the users, who in the Internet experience tend to behave more carelessly and with less discretion. This has been proved in empirical experiments as in [1]. In the most popular social networks millions of users add their personal profiles with the sole intention of communicating news about themselves and gossiping other’s. However, and in the contrary as it happens in ordinary life, all the relationships pass through a single hub which knows –or has access to know– everything.

Thus, when speaking about privacy on online social networks we have to distinguish then two aspects: how to hide or limit the information visible to other peers (a concern also valid in ordinary social life) and how to control the use of the information that the social network provider will make (a concern peculiar of this world). For the first case, social network providers offer the user some configurable settings, in view of their customer´s interest. For the latter case, social networks providers are limited by the law terms and excepting this, they currently use the information as they consider more convenient or profitable. The situation may progress to a state in which online social network users are also aware of this use and start valuing the privacy policies of the site. In this case the use of open standards and clear transactions may enhance the user´s trust in the site and ultimately build customer loyalty to the social network provider.

Online social networks providers always give a privacy policy page in their sites, well visible and which has to be acknowledged by the users at least once at registering time. This web page is in all the cases a narrative expression which perhaps will evolve to standardized forms –just as CreativeCommons symbols replaced verbose texts in copyright statements in Internet resources. Currently the user expresses his privacy preferences by filling in forms (with radio buttons, check boxes etc.) in a configuration page of the web site. The presentation of these preferences and how the site internally represents them remains nowadays variable from social network to social network and far from any standard or pattern. Privacy policy statement actually looks like the transposition of a narrative contract clause from a text paper to a webpage. The authors of this paper envisage that this arrangement may change towards standardized forms. By doing so, the user experience will be improved, the joint use of different online social networks will be boosted and a minimum quality level will be achieved.

This paper is organized as follows. First, a detailed analysis of the current privacy policies used in social networks is presented in Section 2. Then, the different elements involved in a Digital Rights Management (DRM) system are introduced in Section 4; and a brief state-of-art in policy languages is presented in Section 3. Finally, Section 5 analyzes the use of DRM for specifying privacy policies in Social Networks, and Section 6 presents two possible standard-based implementations of privacy applications, one based on a policy language, and the other based on a right expression language.

2. PRIVACY ON ONLINE SOCIAL NETWORKS

2.1 Privacy respecting the social network provider

There is a common set of privacy policies that everyone handling someone else´s personal data must implement: those defined in the law. The legal provisions vary slightly from country to country, but in general individuals are granted with similar rights: the right to rectify the given personal data, the right to be erased from the computer records of the provider´s database etc.

International companies handling personal information which want to operate in the European Union must adquire a certificate: TRUSTe certifies the compliance of the sites with the EU Directive on Data Protection [2]. This Directive prohibits the transfer of European citizens' personal data to companies in foreign non-European Union nations unless they are certified. The TRUSTe seal grants that a site satisfies the seven *Safe Harbor Privacy Principles*, an agreed framework to qualify companies to share information across the borders. The Safe Harbor Privacy Principles constitute a good base to declare what is desired in the privacy prolicies to be implemented by the social network provider, and how can DRM or policy languages help. These principles can be seen in Table 1, as well as its degree of satisfaction by the social network providers.

Table 1. Safe Harbor Privacy Principles in social networks

Principle	Meaning	Satisfaction
Notice	Do social networks inform the users that their data is going to be collected and used?	Yes.
Choice	Do social networks offer to opt out the collection and forward transfer of the data to third parties?	Yes (at least in theory).
Onward Transfer	Do social networks grant that data transferred to third parties will only happen if these also follow adequate data protection principles?	Uncertain.
Security	Do social networks make efforts to prevent loss of collected information?	Yes, but these efforts are unclear.
Data Integrity	Is data used for the purpose it was collected for in the social networks?	Data is used for other purposes too.
Access	Can users access and delete the information social networks have on them?	Mostly.
Enforce-ment	Do social networks provide effective means to enforce the previous principles?	No.

In all of the social networks the principle of *notice* is satisfied: users have to actively declare that they know the privacy policies of the site. Most of them, too, satisfy the *choice* principle, by which they can restrict the data not to be leak to third parties, with a brief reference to how will data be handled after the *onward transfer*. And while it is true that *security* is a concern of social networks providers, there is no mechanism to grant this beyond some vague legal responsibilities. *Data integrity*, as described in Table 1 is in practice not respected at all, given that social network providers reserve themselves the right to use the given data as they consider more convenient. Users can *access* and rectify their data freely (on despite of the threat of Facebook of retaining the data for good). *Enforcement* comes only from the auditing offered by TRUSTe or similar certifying authorities.

The TRUSTe group has certified at least two of the major networks (Facebook and MySpace), who also suscribe other privacy initiatives, like the Children's Online Privacy Protection Act. Audit trails, monitoring and enforcement are granted by the TRUSTe seal, but in practice the control looks somewhat weak. Implementation of the seven Safe Harbor Privacy Principles is irregular, especially in what limits the social network provider data use. It has to be considered that with this paradigm, it is the social network provider the one who has to regulate himself. This commitment at least nominally was assumed in front of the European Commision recently, when a declaration of intentions was approved by some of the major social network providers in Europe[1].

2.2 Privacy respecting other users

Most of the online social networks providers have acknowledged the importance of the privacy policies and besides satisfying the legal requirements they offer their users some advanced configuration parameters going beyond the legal minimum. These extended privacy restrictions are of course offered to protect members from other members, but not from the social network provider themselves.

There is a common consensus around the idea that more control should be given to the users for the privacy matters in the Web 2.0 [3], and it is likely that social network providers go deeper in this matter as long as it does not collide with their business model.

Current social networks allow users to specify who is able to access which pieces of their personal data. In the specification it is sometimes possible to declare which data is disclosed to all, to nobody, to the network contacts or to the contacts of the contacts. This specification can be clearly improved and refined. For example, data could be restricted in function of the age of the recipient user, or the sex, or the country etc. As it will be seen, standard policy languages could be used for this regard.

Open protocols are currently not followed, although a few of the sites allow the user to export their data as RDF (using FOAF, the Friend-Of-A-Friend vocabulary). Worldwide privacy policies standardization is still missing, but this would help the work of the social network owners in order to improve privacy. This good

[1] Safer Social Networking Principles for the EU, on Februay 2009. Site: http://ec.europa.eu /information_society/ activities/ sip/self_reg/social_netwk/index_en.htm

situation in theory is less perfect in practice, and there is still the need for new standardization initiatives easier to implement.

For example, the social network provider servers are secure in front of attacks for their own but none of them takes responsibility to grant their perfect functioning. Thus, each of these networks is liable to suffer virus attacks and data theft while 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.

Thirdly, the terms of privacy also unanimously reflect the exceptions provided by governmental interventions, and for the most privacy paranoics it is not pleasant to be observed at discretion by governments

Some of these privacy flaws might have been avoided with mere technological measures. Information management strategies derived from those already existing in DRM 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. In the next sections, it will be seen how DRM systems and standard privacy policies can help to overcome some of the problems.

3. POLICY LANGUAGES

Policy languages are usually employed to control the access to resources, e.g. digital assets or applications. This is exactly what is demanded in online social networks, so it could be thought that expressing privacy preferences in one standard policy language could allow having interoperability across the social networks and developing Web 2.0 applications in a standardized way. Are current languages operative enough as to serve for this purpose?

Some of the policy languages are the P3P (the Platform for Privacy Preferences [17]), XACML (Extensible Access Control Markup Language [15]) or the "Common Policy", specified in RFC4745 [18] and which defines a framework for authorization policies controlling access to application-specific data. More recently, a W3C group is giving steps towards a new language integrating features of the three precedents (PLING, Policy Language Interest Group [19]).

P3P enables web sites to express their privacy practices in a machine readable format that can be retrieved automatically and interpreted by other agents, like Internet Explorer or Mozilla Firefox. When visiting a P3P-enabled web page, the browser can understand the site´s privacy policies in a simplified and organized manner, and react accordingly to user preferences (for example regarding cookies etc.).

XACML is the language specified by OASIS [10]. This standard policy language was devised for expressing authorization policies in XML, intended to be applied to any object that can be identified in XML.

The XACML standard specifies a policy language model. This model defines the rule element, which is used to define the set of resources, subjects, actions and environments to which the rule is intended to apply. In the rule element also it can be defined the consequence of a true evaluation for the rule, as well as the conditions to refine the applicability of the rule.

The XACML standard uses the W3C XML-Signature Syntax and Processing Standard [16] for providing authentication and integrity protection for XACML policies. The XACML version 2.0 specification provides the model descriptions for data-flow, XACML context (canonical representation of a decision request and an authorization decision), and policy language (rule, policy, policy set). However, in the last term, XACML does not define any rule per se, and this makes an hypotetical interoperability situation among different networks quite difficult to be achieved.

The IETF Common Policy actually defines a very simple XML Schema and expects that the different applications complete it through extensions.

Each of these policy languages looks appropiate to express the user preferences, but they particular profiles for social networks should be specified.

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 [6]. 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. Next subsections describe the elements that participate in a DRM system, compared to their counterparts in social network sites.

4.1 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.

4.2 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 expression languages and policy languages do not differ much in vocation and form.

4.3 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.

4.4 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, as this would detriment the provider´s interest of knowing everything what happens in the network.

4.5 Notification of Events

Some participants of the distribution chain, as content creators or distributors, could want to monitor the 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.

4.6 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 authorization 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 **¡Error! No se encuentra el origen de la referencia.**, and solutions DRM-based (see Section 3) have been already been explored like in [7], where a privacy schema extended the MPEG-21 REL vocabulary and resources were protected by IPMP tools within a security framework.

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, privacy languages also can be used to specify the access rules to user's data (digital assets and personal data). Both, REL licenses, as well as policies can be used in social networks to control the access to users' data. Licenses can be used to govern digital resources and a broad range of rights and conditions can be stated by users by means of one of current RELs and associated to the corresponding resource. However, as they have not devised to control the access to user's data in social networks, probably an extension or profile should be defined for these applications, as done in other environments as the mobile one.

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 [5] 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.

6. SPECIFYING PRIVACY APLICATIONS FOR ONLINE SOCIAL NETWORKS

Most of the online social networks allow developers to create applications that permit users to share content. These applications can be used by other users of the network. In June 2007 Facebook opened a development platform for integrating new applications into this online social network. Facebook allows developers to program social applications, which have available a set of external libraries that enable the access to the functionalities that Facebook offers. These applications basically are web applications, which can be accessed from the Facebook portal. Nowadays, most of these applications are used by millions of people everyday.

Developers can build applications that run on Facebook and let users interact with other users. A user that builds a new application can invite one of his friends to use it, and if she accepts it, then she can use the application within the Facebook portal. The applications are executed in an external server, outside the Facebook environment. The unique direct connection is through libraries and APIs which provide a set of basic functions in the javascript programming language to access to Facebook users data, which includes personal data, photos, messages, etc.

In this context, we have considered the development of an application to control the access to users' data within the Facebook portal. This application will allow users to define more complex access rules to control the usage of their audiovisual material. In this way, it is expected to enrich the privacy concept in online social networks with new conditions of usage. Currently, users can only specify who can access to their personal data in terms of all/nobody, those who belong to groups, to the group of friends, to the group of "friends of my friends", etc. What we propose is the definition of more complex rules as for example "*only my workmates can see the Christmas Dinner photo album during this month*".

As outlined in the previous section, the implementation of this privacy application could be done based on policy languages, or using rights expression languages. Thus, in the following subsections, the specification of these two possible implementations is described.

6.1 Specifications for Implementing Privacy based on XACML

Specifically, we propose to use XACML, previously introduced in section 5, for expressing authorisation policies in social networks. This standard specifies a policy language model. The three top-level policy elements defined for this model are: rule, policy and policySet. The rule element is the basic unit of management within an XACML policy administration point. The main components of the rule element are: the target, effect and condition elements. The target element defines the set of resources, subjects, actions and environments to which the rule is intended to apply. The effect element indicates the consequence of a true evaluation for the rule. The condition element refines the applicability of the rule. The policy element consists of rule elements and mechanisms for combining the results of their evaluation. The obligations element specifies the actions that shall be performed in conjunction with the policy evaluation. Finally, the policySet element enables the combination of separate policies into a single policy.

In the developed application, users can specify and associate more complex access rules to their data, which can be later shared with other users according to the specified policies. One example of an access rule that can be defined using the proposed application is to permit the access to the Christmas Dinner's photo album only to her workmates during this month. In this way, if any other user that doesn't fulfil the specified conditions tries to access to one of the protected photos, the application will not grant him access.

Table 2. Example of a XACML policy to control the access to a digital resource

```
<Policy>
  <Description> Access control policy </Description>
  <Target/>
    <Rule
RuleId="urn:oasis:names:tc:xacml:2.0:example:SR1"
Effect="Permit">
      <Description> Any of Alice workmates can view the
Christmas dinner photo album during this month
</Description>
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name
-match">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string"> Alice
workmates group </AttributeValue>
            <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject
-id"         DataType="urn:oasis:names:tc:xacml:1.0:data-
type:rfc822Name"/>
            </SubjectMatch>
          </Subject>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:ex
ample:vc:schemas:</AttributeValue>
              <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:target
-namespace"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ResourceMatch>
            <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-
node-match">
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/vc:Ch
ristmasDinner</AttributeValue>
                <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ResourceMatch>
          </Resource>
        </Resources>
        <Actions>
          <Action>
            <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">view</
AttributeValue>
              <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ActionMatch>
          </Action>
        </Actions>
      </Target>
       <!-- Only during the January 2010 -->
      <Condition
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
        <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
greater-than-or-equal">
          <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
one-and-only">
            <EnvironmentAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#date"

AttributeId="urn:oasis:names:tc:xacml:1.0:environment:cur
rent-date"/>
          </Apply>
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">2010-01-
01</AttributeValue>
        </Apply>
        <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
less-than-or-equal">
          <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
one-and-only">
            <EnvironmentAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#date"

AttributeId="urn:oasis:names:tc:xacml:1.0:environment:cur
rent-date"/>
          </Apply>
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">2010-01-
31</AttributeValue>
        </Apply>
      </Condition>
  </Rule>
</Policy>
```

6.2 Specifications for Implementing Privacy based on MPEG-21 REL

MPEG-21 REL is defined as a collection of three XML schemata, called the core schema (denoted by the XML namespace prefix "r"), the standard extension schema (prefix "sx"), and the multimedia extension schema (prefix "mx"). These schemata define the fundamental elements of the language, some widely-useful conditions, and elements useful in copyright protection applications, respectively. We present here a suitable privacy extension schema that could be used for implementing a privacy model for social networks (detailed in [12]). The parameterization of this model is based on the following elements: "user role", "recipient", "context descriptor" (information that needs to be protected), "situation", and "precision". The elements of the proposed privacy extension will be denoted by the namespace prefix "px".

First of all, we need to identify the elements already contained in the MPEG-21 REL license that could be easily mapped to the parameters defined in the privacy model. For example, the user who wishes to protect his/her personal information can be easily identified as the MPEG-21 REL *Issuer* (responsible for specifying the privacy policies) while the recipient of the contextual information corresponds to the MPEG-21 REL *Principal* (responsible for exercising the right over some content). Finally, the MPEG-21 REL *Resource* could be used to express a single or even a set of sensitive contextual descriptors that need to be protected.

The most difficult part is to identify how to express the "situation" and the "precision" parameters. "Situation" combines contextual descriptors such as "location", "time", "usage", and "nearby people". We already know, from our previous work in the adaptation authorization [13], that we can include MPEG-21 Digital Item Adaptation (DIA) [14] descriptors inside the MPEG-21 REL *condition* field. MPEG-21 DIA includes the most complete schema for describing multimedia contextual information (user preferences, terminal characteristics, etc). Thus it would have sense to include "location", "time", "nearby people" as MPEG-21 DIA constraints in the *Allconditions* field of MPEG-21 licenses. Nevertheless, to the best of our knowledge, a suitable descriptor does not exist in MPEG-21 to map "usage". Our proposal is to include a "px:usage" element in the conditions field. Finally, the "precision" is expressed implicitly, and hence does not need a special element in MPEG-21 licenses. The issuer of the license is responsible for introducing a more or less detailed description of the context (in the resource field) associated to every principal. For example, the user can define that he allows his family to know that he is in a certain city, but protect the access to the precise geo-coordinates.

It is also relevant to note that MPEG-21 REL defines an element named "r:propertyProcessor" that allows to express groups of principals (users) through roles.

An example of our proposed license based on MPEG-21 REL to govern the use of contextual information is shown in Table 3. It allows the "Family members" to know the "location" of the "User" in order to fix a dinner in the following days.

Table 3. Example of a license based on MPEG-21 REL to govern the use of context

```
<r:license              xmlns:xsi              =
http://www.w3.org/2001/XMLSchema        -instance
xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-DIA-NS
DIA-2nd.xsd  urn:mpeg:mpeg21:2003:01-REL-R-NS  rel-
r.xsd urn:mpeg:mpeg21:2003:01-REL-SX-NS rel-sx.xsd
urn:mpeg:mpeg21:2003:01-REL-MX-NS       rel-mx.xsd
urn:visnet:privacy              drm-privacy-px.xsd"
xmlns:dsig=http://www.w3.org/2000/09/xmldsig#
xmlns:dia="urn:mpeg:mpeg21:2003:01-DIA-NS"
xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS"
xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS"
xmlns:mpeg7="urn:mpeg:mpeg7:schema:2001"
xmlns:px="urn:visnet:privacy"
xsi:noNamespaceSchemaLocation="licenses.xsd">
  <r:grantGroup>
    <r:grant>
      <r:propertyPossessor>Familiy
  members</r:propertyPossessor> <!-- Principal-->
      <mx:view/>   <!-- Right -->
      <mx:diReference>
        <mx:identifier>city</mx:identifier>
          <!--Resource-->
        </mx:diReference>
        <r:allConditions>
          <px:Usage>family dinner</px:Usage>
        </r:allConditions>
      </r:grant>
  </r:grantGroup>
   <r:issuer>
    <r:propertyPossessor>User</r:propertyPossessor>
   </r:issuer>
</r:license>
```

Furthermore, also to the best of our knowledge, there is no real implementation of a privacy protection system based on MPEG-21 REL.

7. CONCLUSIONS

This paper has presented relevant privacy issues in online social networks. Specifically, we have focused on privacy related to the data that users share on these networks taking into account both users' digital resources, e.g. pictures or videos, as well as users' personal data, e.g. contacts, personal information, etc.

First, privacy risks on online social networking applications managing user's personal data have been analysed. Then, we have studied if current DRM techniques are suitable for protecting users' data to finally conclude that some elements of a DRM system, as RELs or protection tools, can be used to protect user's privacy. Finally, we have specified two privacy applications in current social networks. These applications have been integrated in Facebook, since this network provides a development platform for integrating new applications.

8. ACKNOWLEDGMENTS

This work has been partially supported by the Spanish government through the projects MCM-LC (TEC 2008-06692-C02-01) and Segur@ (Centre for the Development of Industrial Technology (CDTI), CENIT-2007 2004, under a subcontract with Safelayer Secure Communications).

9. REFERENCES

[1] Gross, R., Acquisti, A., Heinz, J. H.: Information revelation and privacy in online social networks. In: WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM Press, New York, NY, USA, pp. 71-80 (2005)

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ((EU Data Protection Directive). Authoritative text of the Directive can be found in the Official Journal of the European Communities of 23 November 1995 No. L 281 pp. 0031 -0050

[3] 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)

[4] 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)

[5] International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 15: Event Reporting. ISO/IEC 21000-15:2006

[6] 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).

[7] Sheppard, NP and Safavi-Naini, R.: Protecting Privacy with the MPEG-21 IPMP Framework. In 6th International Workshop on Privacy Enhancing Technologies, Cambridge, UK, June, (2006)

[8] International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language. ISO/IEC 21000-5:2004 (2004)

[9] International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 4: Intellectual Property Management and Protection Componenets. ISO/IEC 21000-4:2006 (2006)

[10] OASIS, Organization for the Advancement of Structured Information Standards, online at http://www.oasis-open.org/home/index.php visited on August (2009)

[11] Bowman, M., Debray, S. K., and Peterson, L. L. Reasoning about naming systems. ACM Trans. Program. Lang. Syst. 15, 5, 795-825. DOI http://doi.acm.org/10.1145/161468.161471. (1993)

[12] Carreras, A., Delgado, J., Rodríguez, E., and Tous, R.: The Impact of Context Information on User Privacy in Social Networks. In IDT Series, vol.3, ISSN:2013-5017 (2009)

[13] Carreras, A., Barbosa, V., Kodikara Arachchi, H., Dogan, S., Andrade, M. T., Delgado, J., Rodríguez, E., and Kondoz, A.M.: Context-aware and DRM-enabled content adaptation platform for collaboration applications. To appear in IEEE Multimedia, 2009.

[14] International Standards Organisation. Information Technology – Multimedia Framework (MPEG-21) – Part 7: Digital Item Adaptation. ISO/IEC 21000-7:2007 (2007)

[15] T. Moses (Ed.): eXtensible Access Control Markup Language (XACML) Version 2.0, Feb. 2005 http://docs.oasis-open.org/xacml/2.0/access control- xacml-2.0-core-spec-os.pdf (2005)

[16] Eastlake D. et al.: XML Signature Syntax and Processing, W3C Recommendation, June (2008)

[17] Cranor L. et al., eds, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation, (2002).

[18] Schulzrinne H. et al., eds, RFC 4745, Common Policy: A Document Format for Expressing Privacy Preferences. (2007)

[19] W3C Policy Languages Interest Group, online at http://www.w3.org/Policy/pling/wiki/Main_Page visited August (2009)