Supporting the users' privacy preferences when sharing personal content

Patricia Charlton[1] and Jonathan Teh[1]
[1] Motorola Labs
Jays Close,
Viables Industrial Estate,
Basingstoke,
United Kingdom
{Patricia.Charlton, Jonathan.Teh @motorola.com)

Introduction and overview of our approach to supporting privacy

The increase in the creation and sharing of distributed multimedia content has led to the creation of new tools and methods to automatically and manually annotate content to assist in multimedia management. The content is often shared within communities and the owner has very little means to protect their content from misuse. This can become a problem when the annotations (metadata) are attached to the content as they provide more personal meaning to the content and thus can lead to privacy concerns. However, there are no tools available to manage content in the way it was intended to be used e.g. carrying privacy preference intention with the content and assisting the user in creating appropriate content access preferences with their community or means to enforce users' privacy preferences.

We are concerned about how to support the user's privacy requirements when sharing multimedia content. Our current user requirements gathering related to privacy and the development of privacy tools have been done within the context of the EC part-funded project aceMedia[4]. The vision of the aceMedia project is to provide the tools to assist in advanced content management. This is to deal with information overload, as users have not just access to content in many forms but also many tools and devices to create all types of content themselves. Management of content becomes increasingly difficult for the user, such as finding the right content, creating collections, annotating content etc.

aceMedia is researching methods to assist in information and content management via knowledge technologies and developments in the Semantic Web. The aceMedia approach involves creating and using metadata to enable intelligent applications such as advanced search and retrieval, personalisation, self-organisation of content, and autonomous content actions e.g. self-determined privacy. The use of metadata does not come without some key challenges itself. Many terms used within the metadata may refer to an implicit informal semantics and do not necessarily provide essential properties or relationships between terms to assist in any automated approach to be applied (the metadata is still useful to a manual approach). However, the move towards the development of ontologies that model domains, preferences, policies and

profiles provide an approach to assist in automating the matching and filtering of content searches.

There are two key trends which require technologies, applications and systems to begin dealing with the complexity of privacy within the digital world:

1. Increase in the creation and use of personal digital content as way of working, socializing and communicating between friends, family and work. This is due in part to the ease by which devices can be used to create and share content, and also in part to affordable technologies and human nature's need to communicate
2. Pressure to address privacy issues and concerns about digital content, to assist users in having control in managing content in the way they would in the physical world

It is worth noting that privacy is not easy to define and requirements come from a number of drivers such as social, legal, cultural and personal views. Hence, any solution that is likely to work will take a more holistic view than just a technological view.

Now that there are many commercial applications enabling users to share content , the need to understand and to support privacy concerns will increase.

Another key factor is to assist in the protection of vulnerable users, who can be exposed to semantic attacks. The potential for fraud will increase as more applications and systems support automation of services, relying more on metadata for integration purposes and the use of profiling for automation of configuration systems.

The idea behind the user centred approach is to give control to users and in the same step, remove complexity.

Supporting Privacy in the Digital World

Two opposing models have emerged from the current debates about the social aspects for data ownership and how this can be used **[1].**

One is the "regulation model" proffered by the European Union (EU) administration. The EU representatives believe that standardized privacy protection regulations (eventually on a global scale) are necessary in order to guarantee security for consumers. Moreover, because security and privacy protection issues concern the status of the individual as citizens before they concern the status of the individual as consumer, these regulations must be developed in the political arena (as the representation of the citizens' will) and then imposed onto the economic sphere. In other words, privacy is regarded as a basic civil right.

The "self-regulation model" is supported by business communities in the USA and the EU as well as the Federal Communications Commission in the USA. This view holds that the best way to secure consumers' privacy in cyberspace is via the virtual marketplace itself. Instead of government regulations, self-regulation is the preferred way to address and enforce the multitude of privacy concerns. In other words, competition and free market will encourage consumers to make deliberate choices, favouring businesses that differentiate themselves by their high privacy protection standards. Under this model, privacy is to be seen as the property of the individual.

Personal information under the regulation model is not treated as a commodity but conceived instead as the fundamental component of privacy. Personal consumer

information, as a result, cannot be exchanged in the marketplace but must be protected from exploitation. The consequence for marketing is that data collection possibilities are clearly delimited and room for interpretation is small. For consumers, it means that their ability to leverage on their personal information in order to negotiate exchange value with the marketer is limited to a minimum.

The self-regulative system allows for complex decision making as to how the marketer should negotiate his or her need for consumer information and the consumer's desire to exchange personal information. Because privacy is defined as a commodity, it can be treated according to the economic laws of the marketplace and without direct normative interference from other authorities. As a result, marketers face a difficult but rich task in managing personal consumer information.

Definitions of Privacy

Patterns of privacy may differ significantly from society to society (see [2]). In other words, what people deem to be private matter depends on social, cultural and political factors. However, while the components of privacy may be a question of cultural particularity, the definition of privacy can be expressed in general terms as the restriction of information diffusion. Here, we follow Alan Westin [3] in our use of the term "privacy," who said that "privacy is the claim of individuals, groups or institutions to determine when, how, and to what extent information about them is communicated to others."

It is not that information is kept out of sight or from the knowledge of others that makes the information or knowledge private. Rather, the information contains matters that it would be inappropriate for others to try to find out about, much less report on, without one's consent; one complains when they are publicized precisely because they are private.

Underlying all the concerns with new technologies is the increased "duration" of communicated data except the one transmitted orally. Once a word is spoken it is gone, except in our memory (which evidently we trust less and less). But information conveyed in written form can be stored in databanks and archives for a long time. Thus, one's concern with privacy is actually one's concern to externalize personal information for a more or less extended period of time. Once our information is outside ourselves it is also out of our control just like the picture taken of us, no longer belongs to us but to the photographer.

Privacy solution based on user preferences

After evaluating the current status of DRM tools and approaches to supporting content access rights when sharing content and evaluating user initial requirements, we designed a privacy preference system using a policy modelling and inferencing approach ([5]).

At a high-level the contextual information is capturing knowledge about the user's privacy. However, the research into many projects and discussions about privacy resulted in many of the findings similar to FIDIS [7], that there was no commonly agreed privacy model and certainly no model related to personal content sharing. Also, systems to-date did not address the emerging P2P trend of content sharing.

From some initial user studies that related to privacy and when sharing content, users had two key concerns: misuse of the content, and the need for ease of sharing with family and friends. The preferences of what to do with content that a user sends or receives are often based on two known facts about the content: who the sender/receiver is and the type of content it is. Resulting from the user studies done so far we summarise the high-level access preferences supported. A user can define preferences:

- When sharing content with anonymous and known communities
- When targeted to a specific environment:
- About specific content
- About specific metadata
- About actions for received content

The user preferences are converted into a policy model. Policies declare explicit actions, taking contextual cues from profiles and preferences. So for example a preference "never share this content" is declared in a policy with an action "grant no access rights" to this content. A further preference example of "share my holiday photos with my family" is declared as a policy with contextual cues, which are "holiday photos and family" (group contacts) with an action "grant access rights" to this content.

We draw upon new developments in policy modelling in web services to support a general model of user policies. We have used Rei [6] to develop our user policy model. Rei provides the general semantic language for capturing the user preferences and privacy rights which is both semantically rich in terms of actions and uniform in terms of structure for knowledge re-use and interoperability. This means that granularity of control over content can be exercised because the policy concept is inherited by all the concepts of the privacy model itself. A core concept of privacy applied here is being able to declare access rights explicitly to digital content. Each user has preferences about how they would like to declare access rights. The access rights and the types of actions to be enabled or disabled are a subset of those that DRM standards support. However, these have been simplified for privacy use based on user requirements and feedback.

To provide the granularity of access rights to different content abstractions and different user perspectives the context of the access rights is declared in terms of contacts, content, metadata and environment.

Summary: Standards and workshop about user Privacy

From standards perspective and the workshop meeting we are interested in establishing:

1. a standard policy language, such as REI, for modelling and handling user's privacy preferences so that the exchange and integration of data across applications can respect these preferences
2. creation of a common privacy model for sets of privacy applications so that the mapping of the users privacy preferences can be handled by the policy language to create consistent and verifiable models
3. creation of standard tools to verify the "privacy model" and " policy language" and to establish a means to provide policy enforcement

Acknowledgement

The authors wish to acknowledge support provided by the European Commission under contract FP6-001765 aceMedia

References

[1] Swire, P. P., & Litan, R. E. (1998). *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*. Washington, D.C.: Brookings Institution Press.

[2] Roberts, J. M., & Gregor, T. (1971). Privacy: A Cultural View. In R. J. Pennock & J. W. Chapman (Eds.), *Privacy* (pp. 199-225). New York: Atherton Press.

[3] Alan Westin, *Privacy and Freedom*, New York: Atheneum, 1967

[4] http://www.acemedia.org/aceMedia

[5] P. Charlton, J. Teh, A Self-governance Approach to Supporting Privacy Preference-based Content Sharing, International Transactions on Systems Science and Applications, Special issue 2006.

[6] Rei Policy Language, http://www.cs.umbc.edu/~lkagal1/rei

[7] FIDIS, Deliverable 2.3, Models and Deliverable 3.3, *Study on Mobile Identity Management*, http://www.fidis.net/486.0.html