PERSONAL AND SOCIAL INFORMATION MANAGEMENT WITH OPNTAG

Lee Iverson, Maryam Najafian Razavi and Vanesa Mirzaee
Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada

Keywords: Personal Information Management (PIM), Social Information Management, Tagging, Privacy.

Abstract: We examine the principles of personal information management in a social context and introduce OpnTag, an open source web application for note taking and book marking developed to experiment with these principles. We present the design motivation and technical structure of OpnTag, along with a discussion of how it supports our design philosophy. We also describe a few examples of how it is actually used, how this usage has improved our understanding of Social-Personal information management (SPIM) principles, and our plans for future enhancements.

1 INTRODUCTION

Information plays a central role in our everyday life. In addition to creating information we often acquire, process, and evaluate existing information to create new sources of information and knowledge. For many, this accumulated information is a central component of their daily life. This collection is often referred to as an individual's Personal Information. The act of acquiring, organizing, maintaining, and retrieving one's personal information is known as Personal Information Management or PIM (Bergman et al, 2004). Nowadays, it is likely that much of one's personal information is stored in digital forms such as electronic documents, email messages, web references and other digital resources usually found within a person's computer system or on the web. In order to manage these digital libraries of personal information resources, people often utilize software systems (i.e. email applications, digital calendars, file systems, and web-bookmark tools) which we will refer to as Personal Information Management Systems (PIMS).

Conventionally, PIM is considered a private activity. However, personal information is often created with sharing in mind or as a result of information sharing activities. This gives personal information management a social dimension, an aspect not properly explored by existing PIMS (Erickson, 2006). However, when people transfer their personal information from a private repository (e.g. one's desktop) into a social space (e.g. the Web) they are typically forced to give up control of some aspects of their information. First, people are no longer free to organize this information in their own terms and are often forced to categorize it into pre-defined taxonomies provided by the particular application being used (e.g. scholarly digital libraries or web forums). Second, people are often limited as to how to define what information (and perhaps to whom) to reveal or conceal.

The recent emergence of Web 2.0 applications as a new trend for managing personal information has created new opportunities for users. These applications not only allow their users to create personal information spaces that are easily accessible from anywhere on the Web, but also give them the tools to organize these information spaces in their own terms, share it with others, and take advantage of others' shared knowledge. Although some Web 2.0 applications are beginning to account for the social aspects of information management (e.g. del.icio.us[i], ma.gnolia[ii]), the relationship between the personal and social dimensions of information management remain largely unexplored in the research literature.

In this paper, we will examine the basic principles of what we call social-personal information management (SPIM) and then introduce OpnTag[iii], an open source web application for note taking and book marking developed by our group to experiment with these principles. In section 2 and 3 we present the design motivation and technical structure of OpnTag, along with a discussion of how

Iverson L., Najafian Razavi M. and Mirzaee V. (2008).
PERSONAL AND SOCIAL INFORMATION MANAGEMENT WITH OPNTAG.
In *Proceedings of the Tenth International Conference on Enterprise Information Systems - HCI*, pages 195-203
DOI: 10.5220/0001689401950203

it supports our design philosophy. We then proceed in section 4 to describe a few examples of how Opntag is used, how its usage improved our understanding of SPIM principles. Finally, section 5 outlines our conclusions and our plans for future enhancements.

2 DESIGN MOTIVATION

The design of OpnTag has been guided by three basic principles:

1. Allowing users to maintain personal ownership and control over personal and shared information,
2. Providing the means for users to share information at different degrees between the extremes of "private" and "public", and
3. Utilizing tagging and intrinsic metadata as primary organizing tools

The following sections provide a more in depth description of each of these principles and the motivations behind them.

2.1 Information Ownership and Control

In today's world, when one engages with an online forum or uses a webmail application or social networking system, there are certain questions that one is often unable to find answers to: who owns the content? Who is exploiting that information to create value? Who is responsible for its care? Is it portable so that I can reuse it in other contexts? Can I remove my information from someone else's control without losing access to the information itself? We believe, in order to build information systems that truly support personal information needs, they must provide a complete, persistent sense of the degree to which information that an individual creates or consumes is his/her own, the amount of control he has over the use of that information, and the ability to properly assess or exploit its value.

This carries over strongly to situations where the information being stored and potentially exchanged is creative, analytic and/or work-related, as now the information itself, the way it is organized and its patterns of use and production have value as personal knowledge. Existing theories of knowledge sharing have compared the exchange of information between people with the exchange of money in economic systems (Fuller, 2002): To have knowledge is to be able to solve problems, predict outcomes, and influence others. All of these have great economic potential and in our "knowledge economy" it is the content, organization and control of one's knowledge that creates economic advantage for both organizations and individuals. Even though moving local information into online repositories often implies sharing with groups beyond users' control (e.g. see Amazon's Terms of Use), people are often willing to do so for two reasons: 1) online tools provide significant enhancements in utility and cost (e.g. Google Mail is free, intuitive, reliable and available anywhere) over similar desktop tools; and 2) it becomes remarkably easy to share information and generate an audience when you choose to put that information and knowledge online. These two advantages are in many cases so strong that users are either explicitly willing to give up control of that information or do so without any real awareness of the degree to which they are doing so.

An ideal solution to this problem would be a system for managing personal information that had the advantages of local storage systems in terms of control over organization, access and exploitability, but that was managed online where it could be easily shared with others. Researchers have long imagined and indeed built network-base "data banks" that safely store and manage personal records (e.g. health data banks), but have largely left unexplored the issues of manipulation, organization and personal control over those records. One of the main motivations behind the design of OpnTag then has been to create such a data bank, but with unambiguous personal ownership and control of the information stored in it.

2.2 Different Shades between "Private" and "Public"

When we examine the new generation of Web 2.0 systems as SPIM tools the gap between their personal and the social aspects becomes obvious. Clearly, when using such tools users are aware of both the personal utility and social projection of their information (Marlow et. al. 2006). However, other research suggests that when personal information is shared with a group, the way it is used and managed changes (Erickson, 2006), and both the nature of the information and of the group are critical to these changes. This highlights the need for users to be able to define and manipulate the sharing contexts. In particular, personal artifacts managed by SPIM tools may span a wide range of types, from ones' contact information and interests to his/her social network, scholarly work, and opinions. These kinds of information may be public, private or selectively shared with well-defined and understood

groups, and the sharing may happen in a variety of contexts, for example competitive as well as collaborative. Furthermore, the nature and state of these personal artifacts, the group with which they are shared, and the relationships between the owner and the receivers of information are all dynamic (i.e. drafts become publications, people join or leave a group, and users change team/projects) (Razavi and Iverson, 2006). We claim that this combination of context-sensitivity and dynamicity makes both the public/private dichotomy (as seen in many Web 2.0 systems such as del.icio.us) and static access control models (derived from file system and enterprise service security models) inadequate for SPIM applications (Razavi and Iverson, 2007).

In the SPIM domain the information sharing act is often about establishing and maintaining a dynamic sharing relationship: users have nuanced ideas about what they want to share with whom in what context and rather than a binary scale of public vs. private, their judgment of the privacy of their resources often reflects a transition from private, to semi-private/restricted share, to public, depending on the state of the artifact, the group in which it is shared, and the context of sharing.

An underlying user interaction model must then take into account that at any time during an artifact's life cycle, artifacts' categorizations might change; users' need to share classes of artifacts with certain audiences might change; and user's relationships and trust patterns within those relationships might change. Finally, users come to expect their tools to provide flexible support for these changes in their privacy preferences when the social parameters that define the sharing model change (Razavi and Iverson, 2006).

From a user's point of view, the primary concern in managing information sharing is the ability to define the audience that will have access to their information. A simple example is the case of contact management, in which users selectively choose which of a variety of different categories of 'friend' and 'colleague' will be allowed to contact them in a particular way (e.g. who do I give my phone number, address, or AIM id to?). Without aid of technology, we either publish them for all to see or hand them out individually or in particular contexts (e.g. I tend to give my cell phone number to students I teach, but not other students). Generally, the choice of audience for a particular artifact or personal attribute is expressed in terms of a group of others who one trusts with that particular piece of information, so tools should provide support for the definition and manipulation of these groups in which information is to be shared.

Traditionally, group definition for access control has been based on organizational roles (i.e. RBAC (Sandhu et. al., 1996)) or the equivalent (i.e. task (Thomas and Sandhu, 1997)). While it makes sense for an organization to align access rights to organizational roles, it makes little sense for a user to align privacy rights with those organizational roles especially when their members are managed by others. In the social networking world, access is often defined in terms of 'networks of friends' relationships, in which all `friends' are created equal and are often required to be reciprocal (e.g. in Facebook[iv]). But when dealing with information privacy in the SPIM domain, the potential audience for personal artifacts or attributes must be defined in a user's own terms, based on a variety of kinds of relationships, some of which are one-sided. As such, our second design motivation has been to enable users to define egocentric groups of friends or collaborators and then enable them to assign access rights to their personal information based on these user-controlled relationship models. We will describe how Opntag handles this need below.

2.3 Tagging as Primary Organizing Tool

Finally, we approach the issue of information organization. Long one of the most difficult and problematic issues for PIM systems, it has been long obvious that neither traditional filesystem models (i.e. files and folders) nor newer semantic approaches were adequate for managing a wide range of kinds of information (as seen in PIM systems) in a cohesive, intuitive and user-centered fashion. Recently, however, Web 2.0 applications (in particular del.icio.us and Flickr[v]) have presented "tagging" as an incremental, user-centered strategy for organizing personal information in a public space.

The web bookmarking service del.icio.us first introduced tagging to a broad audience by asking its members to submit a list of words along with any bookmark to be saved. Any word or set of words can be associated with a bookmark and they form the fundamental organizational structure of the system. In essence, each tag that I use becomes a "category" within my own information space and since I can use as many tags as I want for each item, I place any item in as many categories as makes sense to me.

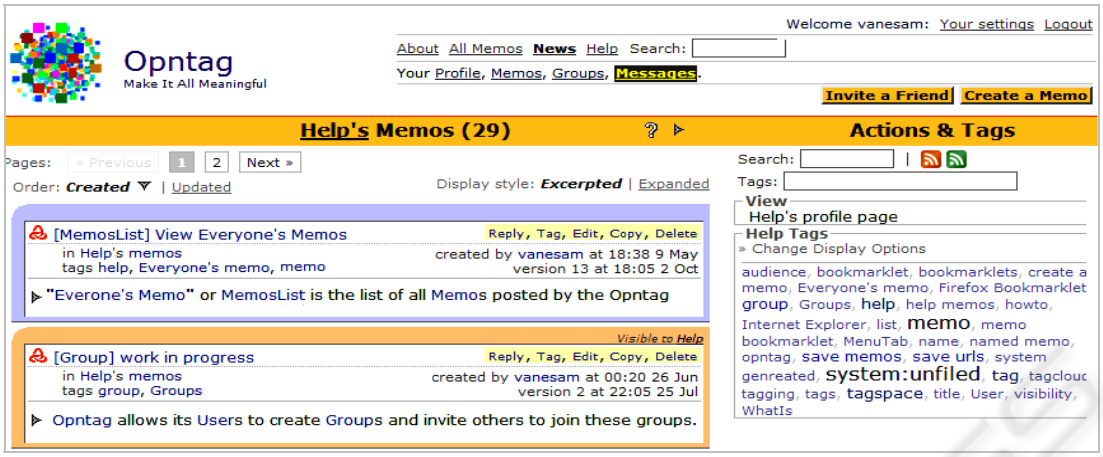

Figure 1: Opntag.

Moreover, tagging plays out socially by allowing me to see other's bookmarks and tags, to see what resources have been tagged the most, and who else has tagged the same items I have or has used the same tags. In other words, it simultaneously solves a wide array of different issues with personal and social information organization such as multiple categorization, recommendation and even the discovery of like-minded others, all without imposing any top-down "correct" organizational model on any user.

Unfortunately, tagging alone seems insufficient. For one, there is a great deal of other metadata associated with PIM resources that is potentially exploitable (e.g. when items were tagged, viewed, modified, copied or used and by whom). It is for that reason that we suggest that the tagging model be augmented by detailed tracking of these events (the "behavioural" metadata for the system) and an integrated ability to exploit them. In essence, we suggest tagging as the key deliberate organizational model and the exposure of passively created intrinsic and behavioural metadata to augment this. Therefore, we designed Opntag tagging classification model with these principals in mind.

3 OPNTAG CONCEPTUAL MODEL

The main purpose of OpnTag is to facilitate creation, organization and consumption of information and knowledge for an individual operating in a social environment. The fundamental unit of information storage in OpnTag is the 'memo', a tagged textual annotation that may optionally link to a web resource. Users create memos to save notes or bookmark URLs, browse and tag other users' shared memos to mark their interest in them, and reply to other users' memos to create a conversation. Another important component of Opntag are *Groups*. Opntag users can use groups to define various communities to collaboratively create and manage information and knowledge. The following sections present a brief description of Opntag's key concepts.

3.1 Memo

A Memo is the basic unit of memory in Opntag. It has a Name or Title, an optional Link (URL) specifying what it is "about", a set of Tags, and some text (its content). It is owned by an individual or group and has a potentially restricted audience (described below). Memos can function as bookmarks, notes, or web pages and are organized based on their intrinsic metadata (e.g. who owns or created them and when) and tags applied by various users.

Memos have globally unique system-assigned IDs and may have a user-assigned Name which is unique among all memos owned by the same user or group. This unique name can be used to refer to that Memo in a more meaningful way than the ID, either when linking from another Memo (using a "named reference" shorthand), or when providing a URL. For example, when one wants to refer to a named Memo within Opntag, one only needs to provide a reference to the Memo's owner and Memo's Name (e.g. a link to Folksonomy in Leei's Space is written as [[Leei:Folksonomy]]). This will create a hyperlink to that named Memo. This gives Memos a Wiki-like functionality (the ability to refer to pages by name). Like Wiki pages a Memo does not have to

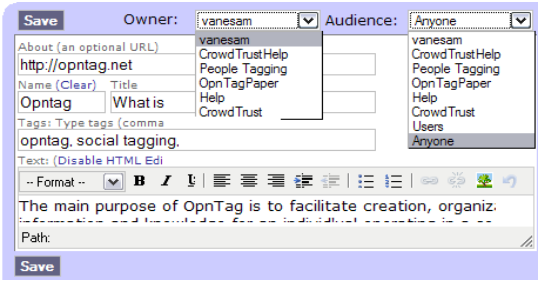

Figure 2: Memo.

exist to be referred to, following a Memo's name link actually opens a dialogue to create the Memo if it does not exist. With this in place, OpnTag enables its users to easily create both individual notes and bookmarks and networks of cross-referenced information units.

3.2 Tags & Spaces

Opntag provides its users with personal and social information management workspaces (referred to as "spaces"). A space is a workspace within which a single User or the members of a Group (see below) can work to create, edit, and organize a body of information consisting of memos and associated tags. Opntag utilizes tags as a lightweight and flexible way to organize, contextualize, and represent Memos.

A User's personal Space contains all Memos created, edited, or tagged by the User and a set of tags associated with these Memos by the User (refer to as User's TagCloud). A Group's Space includes any Memos specifically in that Space or specifically visible to that Group and their associated tags along with the Group's TagCloud (a Group's TagCloud is a collection of tags associated with Memos owned by the Group).

Within a User's Personal Space only that User may create, edit or tag Memos whereas within a Group's Space, any member of the Group may do so. By placing a Memo in a group Space, all members of that Space can edit it.

3.3 Navigation & Grouping

As in other tag-based systems, objects in Opntag are grouped based on ownership and tagging. Users initially have access to all memos (as restricted by the memos' visibility) and from there can select subsets by filtering based on an ownership "space", a tag or set of tags, or some combination of those (e.g. all Leei's memos tagged "rails" and "javascript"). Thus these attributes of a memo, both the intrinsic metadata and user-supplied tags, both identify and group memos. The navigation model depends on selecting these filters via hyperlinks (thus each set of filters is represented by a distinct URL) and adding and removing filters based on links created and presented in each display context. The tagcloud described above is one such context.

3.4 User

A User is an individual who has an account with Opntag. Being a personal information management application, Opntag provides each User with a personal Space where s/he has complete control as how to organize, represent, and share information. Users are the only ones who can create, edit, tag and delete Memos within their own personal Space.

3.5 Group

A fundamental goal of OpnTag is to provide selective sharing, which is supported through creation and management of groups. The primary function of groups is to allow a set of people with a shared interest to create a context for selectively sharing personal information and a collective space within which they can actively collaborate to create, edit and organize information either publicly or in private. Because groups have their own views of entries assigned to them and their own tag lists, a group can be a very convenient way for sets of people to get a more focused view of their data than by searching or browsing through the main page. If one group is made a member of another (a subgroup relation) then all of its members are necessarily members of the enclosing group (a nested set relation). A number of special groups exist: "Users" which includes all individuals registered with the OpnTag instance, "Unknown" which includes the anonymous, unregistered user, and "Anyone" which includes both groups and thus represents truly public access.

With individuals and groups, OpnTag's access and privacy control centre around the joint concepts of ownership and audience. For each memo, the creator can specify the memo’s owner, which controls who owns the memo and thus can edit and delete it, and its audience, which controls who can see that the memo exists and read it. In OpnTag, visibility implies readability, so there is no “I can see that it exists but can’t read it” issue. The audience for a memo can be either set to the owner (either an individual user or a group) of the memo, or to any super-group of that, including "Users" and

"Anyone", which are super-groups of all others. Only the creator can modify ownership, but any member of the owning group can change a memo's audience. This audience restriction is thus the fundamental privacy control in OpnTag, and it is determined either individually or collectively. It can be set or modified for a variety of different objects and attributes besides memos in OpnTag (such as profile entries and tags), but for simplicity of description we will mention only memo audience in the discussion below.

OpnTag supports two types of groups: *Classic groups* and Egocentric *groups.*

3.5.1 Classic Groups

Classically, a group is defined as a set of people with a common interest and membership in a group is voluntary. This mirrors the "group" model provided by systems such as Google or Yahoo groups and is directly supported by OpnTag. Users can choose to be members of as many such groups as they want, and can create as many groups as they want.

Membership. At the moment, group membership is by invitation: each member of the group may invite as many people to the group as s/he wants by sending an invitation to their email address.

Visibility. For each group created, the creator specifies the group's visibility (one of "Members Only", "Users", or "Anyone"), and the visibility of the member list (same options as group visibility plus "Private", meaning no one would know of user's membership in the group except for the user himself). Of course, the visibility of the memos, tags and member list of a group is restricted by the visibility of the group itself (e.g. it is not possible to make a group visible only to its members, but make its member list visible to anyone). By using various combinations of group and members list visibility, users can create groups with different dynamics and then restrict the visibility of their memos or profile items to any of these groups, including the 'private' group consisting only of oneself. With these variations available, we hope to be able to investigate how trust and sharing behaviours can vary depending on the visibility and dynamics of the sharing context.

Administration. Currently, all group members have equal administrative rights, which include creating subgroups, inviting new members, tagging within the group, and editing, deleting and changing the visibility of any group-owned memo. Groups can be destroyed only if they have no memos and only by the group's creator.

3.5.2 Egocentric Groups

In addition to these "classic" groups, OpnTag also supports a different type of group called egocentric groups. Egocentric groups primarily provide support for relationship management and are handled by tagging people through their profile pages. When visiting another user's profile page, a user can tag the profile with keywords that represent his/her perception of that user or their relationship (i.e. a teacher might tag their students as "student" or "grad student"). In the same way that tagging resources both identifies and groups them (e.g. all memos tagged "rails" can be treated as a group), each such "people tag" represents a relationship group that is usable as a privacy control feature. When creating self-owned memo, the user has access to both his group memberships and his relationship tags and can thus set the audience of the memo to either a group he is a member of or one of these egocentric groups. Thus he can adjust his audience to either one of the groups with collective membership dynamics or one over which he/she has complete control. Again, we plan to investigate the implications of this for trust and sharing behaviour.

Membership. People tags are assigned and removed only by the tagger. As such, the relationship groups that are created as a result of people tagging are entirely controlled by the creator; meaning people do not need to agree to be in the group, and they may not even know that they are included in a certain relationship group. An important implication of users being able to assign their acquaintances to different relationship groups (potentially without their knowledge or approval) is the opportunity for handling many social situations that can be hard to handle in social networking systems (e.g. discretely concealing exclusions when necessary).

Visibility. Each new tag applied to a person has a distinctly specifiable visibility. The choices for people tag visibility include only the tagger, only the taggee, only the set of people tagged with the same tag (by the same tagger), "Users", and "Anyone". Significantly, a single tag may have different visibility to different taggees (e.g. a man might tag multiple women with "girlfriend" so that each only sees their own tag), but in no case can the tagger make a tag visible to anyone other than the taggee without also making it visible to the taggee himself. Since all such tags are visibly attributed to the tag creator, this design choice was made to discourage antisocial tagging by forcing such taggings to be exposed to their subjects (e.g. I can't let my friends

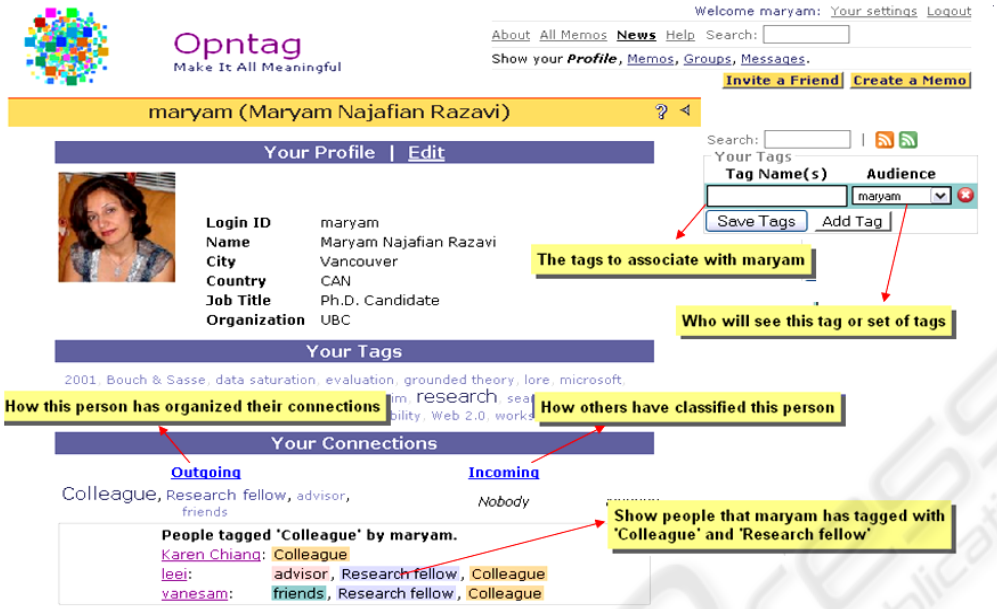

Figure 3: Creating Egocentric groups.

know that I've tagged someone as a "jerk" without letting the "jerk" know too).

Administration. Unlike classic groups, egocentric groups are controlled entirely by the creator: the acts of creating or deleting a tag on a user, and controlling the visibility of the tag are solely controlled by the tagger and easily modified. We believe that this makes the act of people tagging lightweight and suitable for handling the dynamics of relationships that frequently show up and fade out in natural social environments, but can be difficult to manage online.

3.6 Messages

To support consumption and management of information (and knowledge) Opntag automatically notifies its Users of the activity in their Spaces (either personal space or group space) through "Messages". The "Messages" page contains a list of of such notifications for the User from the System. These messages are created whenever others create, update, tag, delete, or reply to a Memo within a Space of which the user is a member (e.g. so-and-so created or modified a Memo in one of your Spaces, or so-and-so replied to one of your Memos). The User can see the Memos referred to and manage these notices as one might manage email (ignore etc.).

4 USAGE

Since its release as part of GUSSE[vi] demonstration in June 2005, OpnTag has been adopted by over 100 users. In addition to individual usage, various groups have been using OpnTag for educational or organizational purposes. Here we present two experiences of deploying OpnTag in real world situations. We discuss the scenarios, the feedback, and the changes we made to the design as a response.

4.1 CrowdTrust

CrowdTrust[vii] is a small start-up focused on creating collective intelligence solutions and active in the development of OpnTag. The company has 8 members, including designers, developers, marketers, and CEO. The CrowdTrust team has been using OpnTag for information management and sharing within the organization for over a year. Separate groups have been created to serve different information sharing purposes: the "CrowdTrust" group is the main group that all the corporate staff are a member of. Issues relevant to all team members such as meeting plans and agenda, meeting minutes, competing companies, similar products, and potential customers are shared between staff by creating memos either in the CrowdTrust space, i.e. in situations where any CrowdTrust member is expected to contribute; or in member's personal

space visible to CrowdTrust, so that other CrowdTrust members can also see it. There are also two other groups, each with a selected subset of corporate staff as members: "CrowdTrust Help", used by developers for communicating help materials on company's product to the customers; and "CrowdTrust Board", used by company board members for discussing management issues.

The CrowdTrust experience has helped us clarify which features of the application users appreciate the most and which parts of the interface are confusing to them. We have not done a formal usability study in this context, since many of the users are also system developers, but it has been clear that for at least some of us, engaging with the tool has become an essential daily activity and valuable resource. It is also clear that engaging with both the privacy control and tag-based organization is simple, natural and no great barrier to usability.

4.2 ETEC522

In the fall of 2007, OpnTag was used as the main course information and interaction system for ETEC 522, an online course on educational technologies offered by the University of British Columbia. Students used it for both their own information management within the course and for conversation and sharing resources with the rest of the class. Throughout this process, we had no negative feedback with respect to the privacy or information management aspects of the system.

The major criticisms from use in this context were centred on the management of conversation and awareness using the tool. At the start of the course, when students asked for the memos for the group "ETEC 522", the system would select those memos "owned" by the group. It was clear that this was inadequate, in the sense that the students expected that specifying the audience of a memo for "ETEC 522" would also have the effect of it being seen in the group "space". After this, we revisited the selection of memos considered to be part of a "space" (for an individual or group) and realized that there are various ways of both claiming a memo for oneself and providing it to a group. Currently, when visiting an individual's space the memo set includes all memos created, modified or tagged by that user. When visiting a group's space the memo set includes memos owned by the group, tagged in the group and memos made explicitly visible to the group. Moreover, OpnTag's message system notifies all members of a group when any of these memos are created or modified. In this way, membership in the group now allows one to both contribute to and monitor the group in a variety of ways.

5 CONCLUSIONS AND FUTURE WORK

In this paper, we presented Opntag, an online, open source web 2.0 personal and social information management application. The primary design motivation behind Opntag is to support fluid organization and sharing of personal and social information. We attempt to accomplish this by:

- allowing individuals to maintain control and ownership of their information in both their personal and social spaces.
- supporting the creation of various communities where members can collaborate and selectively create, manage and share information
- adopting a tag-based organizational model and augmenting it with intrinsic metadata to support better exploitation and navigation of the space

Like many other web based applications, OpnTag is constantly being updated and improved upon. Functional updates can be very frequent – sometimes even occurring daily. In addition to these minor modifications, we are currently pursuing a number of larger extensions:

1. Managing the space between audience control, which bounds the audience for any particular item or conversation, and audience notification, which makes the audience specifically aware of certain activities. We are currently extending the notification model to allow more specific control by both information producers and consumers of the streams of notification information managed by OpnTag. This work is motivated by feedback received during the ETEC5221 user study.
2. Creating a semantically rich tagging classification model by providing Opntag's users with the means to construct relationships between tags in a way that is meaningful to them. For example, I might state that my tag ‘CSCW’ will automatically be added to any memos tagged with both ‘email’ and ‘research’. This will allow us to make the transition from tag relationships (e.g. “related to”) that are trivial, un-interpreted, and mechanistic, to tag structures that are rich, user-interpreted, and personally created. We believe that creating more complex relationships between tags will allow Opntag’s users to not only create

collections of information resources that are more refined and have deeper context but will also enable them to create information spaces that are easier to navigate and explore.

REFERENCES

Bergman, O., Boardman, R., Gwizdka, J., and Jones. W., 2004. Personal information management SIG. In *Extended Abstracts of CHI 2004*. ACM Press. pp. 1598-1599

Marlow, C., Naaman, M., Boyd, D., Davis, M., 2006. Tagging Paper, Taxonomy, Flickr, Academic Article, ToRead. In *Proceedings of Hypertext 2006*, New York: ACM Press.

Erickson, T., 2006. From PIM to GIM: personal information management in group contexts. In *Communications of the ACM*, January 2006

Fuller, S., 2002. *Knowledge management foundations*, Boston: Butterworth-Heinemann

Razavi, M. N., Iverson, L., 2006. Design guidelines for an information privacy management system for personal learning spaces. In *Proceedings of e-learn 2006,* Honolulu, Hawaii, USA

Razavi, M. N., Iverson, L., 2007. Designing for privacy in personal learning spaces. In *New Review of Hypermedia and Multimedia,* In press.

Sandhu, Ravi S., Coyne, Edward J., Feinstein, Hal L., & Youman, Charles E., 1996. Role-based access control models. In *Computer*. Volume 29, Number 2, pp 38-47.

Thomas, R., Sandhu, R., 1997. Task-based authorization controls (TBAC): Models for active and enterprise-oriented authorization management. In *Database Security XI: Status and Prospects*, North-Holland.

[i] http://del.icio.us
[ii] http://ma.gnolia.com/
[iii] http://sourceforge.net/projects/opntag
[iv] www.facebook.com/
[v] http://www.flickr.com
[vi] http://gusse.org/
[vii] http://crowdtrust.com/