Analysis of Collective Privacy Decisions in Social Computing Sites

Nicole DeSisto

State University of New York at Brockport

Abstract

This paper focuses on issues of collective privacy management in social computing sites. We begin with reviewing previous research on privacy issues and their proposed solutions on social networking websites. Next, we analyze the current collaborative privacy features on state of the art social networking sites and propose three different collaborative privacy tools that could be implemented on these social networking sites. Lastly a survey was conducted presenting these three tools to 82 participants on Mechanical Turk to see which type of group privacy settings users of social networking sites would prefer to have implemented.

Analysis of Collective Privacy Decisions in Social Computing Sites

Introduction

Social computing is ever increasing in popularity, and with this growth there has been an increase in the number of privacy breaches caused by the sharing of information across these websites. This has caused numerous people harm, especially in working environments (i.e. colleagues or employers with access to personal material posted on these social networking sites). Certain uploaded images have caused people to lose their jobs, or lose job opportunities from potential employers. People have also been put into embarrassing situations by their friends, family, or significant others. Most of these instances involve uploaded photos of the user at a party, club, or drinking alcohol. Most research in the area of privacy issue control has been on the individual level, and there has been a consensus that users desire more privacy control over their information, but little has been done in the area of collective privacy control and on what types of control features users would be willing to use. Users of social computing sites want the ability to control who has access to view the information that is linked back to them. This could be in the form of videos, photos, or text. This paper investigates this problem, and focuses on issues of collective privacy in the case of co-shared photos. We conduct an exploratory study involving 82 users of social networking sites and three simplified collective privacy tools.

State of the Art

This section will review related works, with emphasis on privacy issues on social computing sites. We focus our analysis on three recent works, which discuss the current state of individual privacy settings on popular social networking sites, and the way users cope with the current limitations on privacy settings of these sites.

It was reported in that users of social networking sites felt it would be troublesome to control disclosure on social networking sites thoroughly, though they differed on the amount of effort they were willing to invest in managing privacy [1]. Users desire easy, simple-to-use, or automated interfaces to remedy privacy issues. The more complicated or time consuming the privacy preserving mechanism is, the less likely users are to accepting it [2]. Privacy was the highest concern for content (specifically photos) that captured memories, or were culturally embarrassing/frowned upon [2]. Users also reported different expectations and tolerances between various social circles, according to their culture or generation [1].

One of the most interesting findings was the conflicting desires for shared content. If a user is tagged in a picture, they believe they should have co-ownership rights to it, but if they are the owner of a picture and someone else who was tagged requests co-ownership, they are less accepting of the idea [3]. Interestingly, Besmer and Lipford found that there exists stronger concerns with user content being visible to specific individuals in existing social circles, and there isn't as strong of a concern with strangers viewing personal content [3]. Lastly, all the reviewed papers came to the conclusion that personal privacy policies are often highly dynamic and may vary depending on the current context, need, or activity.

Current Technological Affordances of Social Computing Sites

This section summarizes the major findings found to be in common on individual and group privacy policies on the current top fifteen social networking websites.

Our study uncovered that in all current social networking sites, the person who uploads a piece of content is the owner of said content. As such, the owner is the only one who can remove the image or set privacy settings on the content. Subsequently, no existing social networking site has an effective way for users who are tagged in content to remove or hide said content. There are also currently no co-ownership features available. Interestingly, our analysis also revealed that current technological affordances are not related to the popularity of the site: Facebook or Google, for example, do not appear to support more advanced collaborative privacy features than smaller niche sites, wherein the notion of groups is more emphasized. In fact, we found that groups are a common features on all sites, and most active in smaller communities, wherein sharing is the norm.

In the table below, named websites are the sites found to have the most advanced collaborative privacy features available on current social computing sites and their features are noted.

Site Type	Groups Support	Collaborative Privacy Settings	Administration Among Groups	Shared Resources	Interaction Level within Groups
Blogs/Communities (LiveJournal, Reddit)	Yes. These have the most support or development of groups.	Reddit allows members of groups to report content posts to moderators.	Owner and appointed moderators only.	Pictures, videos, blogs	Highest level of group interaction because these sites have more focus on content sharing in their groups. The size of the groups range.
Professional Networks (LinkedIn)	Yes. These groups are usually based on professional or educational goals.	LinkedIn group members can flag items as inappropriate. This will add the content to a moderation queue, or if chosen by moderators, will delete the content outright after a set number of flags are sent in.	Owner and appointed moderators only.	Personal information, locations	Varies. Some users choose to be active in groups and others join to just support the group's cause.
Social Networks (Facebook, Google)	Mixed. Sites more focused on dating have a tendency to not support groups. Popularity of the site doesn't seem to have any correlation to group support.	None.	Owner and appointed moderators only.	Pictures, videos, music	Least amount of interaction because of the other focuses on the networking sites besides groups. The groups tend to be very large.
Content-Specific Sharing Sites (DeviantArt, CafeMom)	Yes. DeviantArt and CafeMom support them.	Admins on DevienatArt can make sub areas in their group that are only visible to those in a designated membership level.	Owner and appointed moderators only.	Pictures, videos, blogs	Higher than social networking sites but less than blog/communities.

Table 1 Summary analysis of the key features in current social computing sites.

Study

Based on our analysis of state-of-the-art social computing sites and relevant literature, we have conducted an exploratory study in order to determine possible methods to fill the identified gap in the access control mechanisms currently available.

Methodology

We recruited 82 participants from the Mechanical Turk (www.mechanicalturk.com) web portal. Participants were given 0.25 cents per task. Mechanical Turk is crowdsourcing internet marketplace where "requestors" can post HITs (Human Intelligence Tasks) for "workers" to complete where human intelligence is needed to perform tasks that computes are currently unable to do. We presented the participants with a video on three different collective privacy tools that could theoretically be implemented on current social networking websites. The three scenarios are referred to as "censor bar", "keyword tagging", and "group agreement". The three scenarios are explained in detail in the section below.

Minimal User Collaboration: Censor Bar Scenario

When a user is tagged in a photo, they have an option of putting up a censor bar covering their face from other users. They can customize who sees the censor bar based on friends or groups of friends and it can be edited at any time by the tagged person.

Medium User Collaboration: Keyword Tagging Scenario

Users create lists of friends based on who they want to be able to view certain types of photos, this is built around a set list of predefined keywords (ex: party, work, home, family, outing, vacation, holiday, artistic, animals, etc.). When a user uploads a photo, people in the photo are tagged and the photo is also tagged with words that describe the photo from the keyword list. This then automatically sets the privacy for the photo based on the keyword tagging. Example: No people in the "family" group can see photo's tagged with the keyword "work").

Maximum User Collaboration: Group Agreement Scenario

When a user uploads a picture and tags all the users in the photo, the photo is put into a temporary negotiation area where no other users can view the picture except other tagged users. Those users, who were tagged, suggest who they want to be able to see the photo. All users involved put forth who they want to be able to see the photo and they can choose those from the other user's friends who they do not want to see the photo. Once everyone is at an agreement, the photo is uploaded with those privacy settings. Any changes a tagged user makes notifies the other tagged user and they have to negotiate the photo's privacy settings again.

After viewing a short online video exemplifying these three collaborative privacy scenarios the participants were given a survey to investigate their perception and obtain feedback. The survey questions focused on answering the question of what type of collective privacy features users of social networking sites would prefer to use if actually implemented - which types of collaboration they found practical and impractical for privacy control.

Results

Participants were on average between the ages of 25-34 (std. 1.080). 50 were male, 30 were female, and 2 did not answer. Participants accessed social networking sites on average of once a day (std. 0.575) and they uploaded photos to these websites on an average of once a month (std. 1.075). As seen in figure 1 and 2 below, the scenario participants found to be the easiest to use was Keyword Tagging, and the most difficult to use was Group Agreement by a large margin.

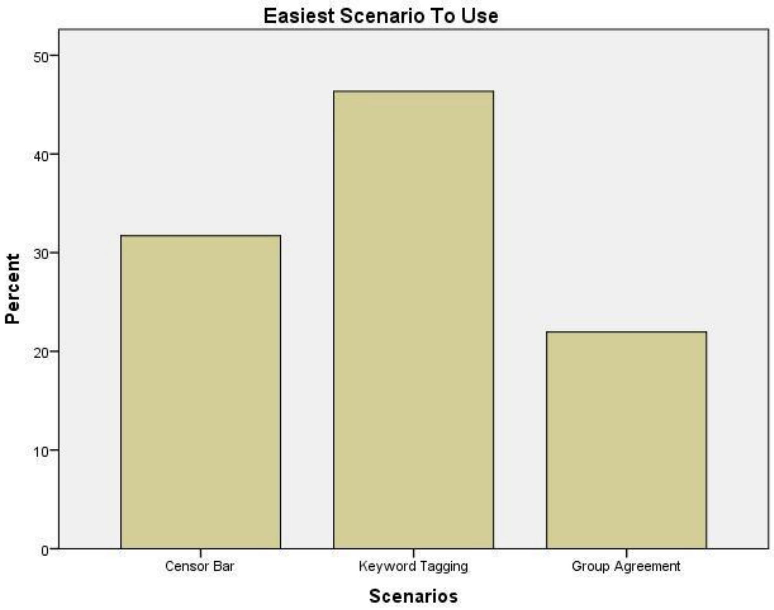

Figure 1 The scenario participants found easiest to use.

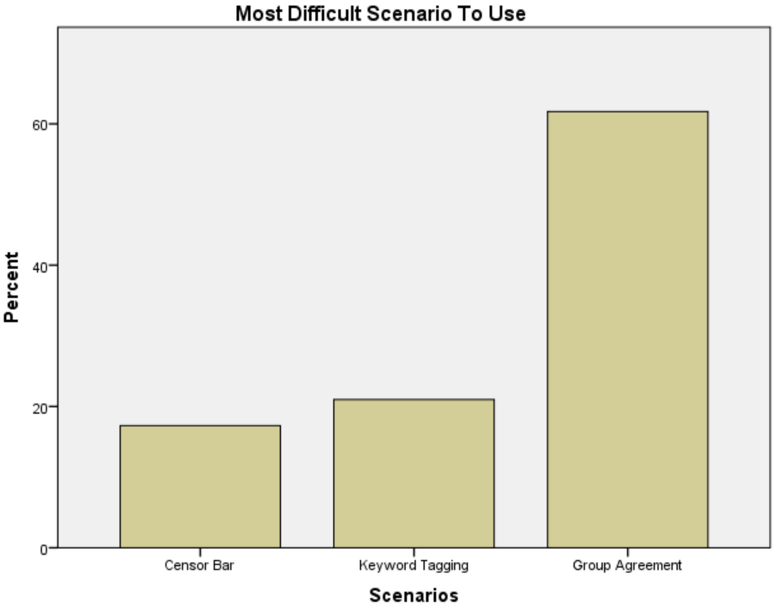

Figure 2 The scenario participants found most difficult to use.

Participants also found Group Agreement to be their least liked when it came to which scenario they would not prefer when uploading many photos at once, with 47.6%

disliking Group Agreement. They preferred Keyword Tagging for optimizing the uploading tasks (48.8% participants).

When it came to which scenario participants considered fairest, two different questions were asked. "Which scenario seemed to be the fairest approach in deciding the privacy settings of photos that you have uploaded, that have other people tagged in them?" And "which scenario seemed to be the fairest approach in deciding the privacy settings of photos that you did not upload, but you were tagged in?" These two overlapping questions were added to assess whether participants had different opinions on collective privacy when they were the owner/uploader of the photo versus a photo owned by another person that they were tagged in. Interestingly, users held an almost equal opinion of Keyword Tagging and Group Agreement when they were the uploader, 35.4% for Keyword Tagging and 37.8% for Group Agreement. However, when someone else was the uploader, the amount of participants who liked the Keyword Tagging scenario decreased sharply to 22.0% approval of Keyword Tagging versus 42.7% approval of Group Agreement. Another question was asked "In the scenario using keyword tagging, how likely do you think people will tag photos with the proper keywords?" And that resulted in fairly positive answers toward the likelihood of proper keyword tagging in the Keyword Tagging scenario, as seen in the figures below.

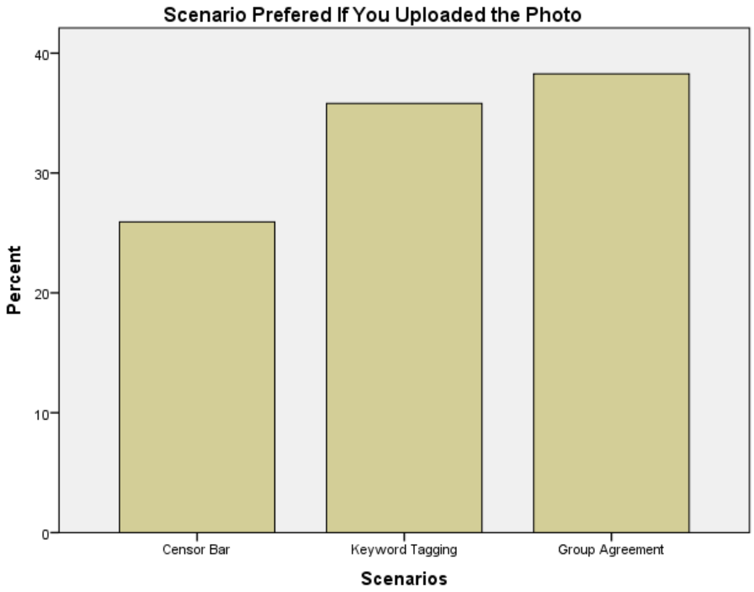

Figure 3 The scenario preferred by participants if they were the owner/uploader of a photo.

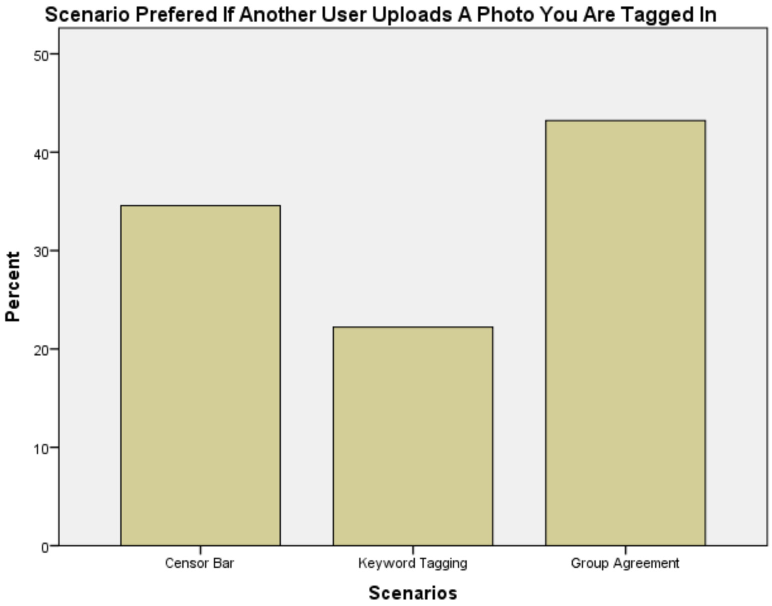

Figure 4 The scenario preferred by participants if they were tagged in a photo uploaded by another person.

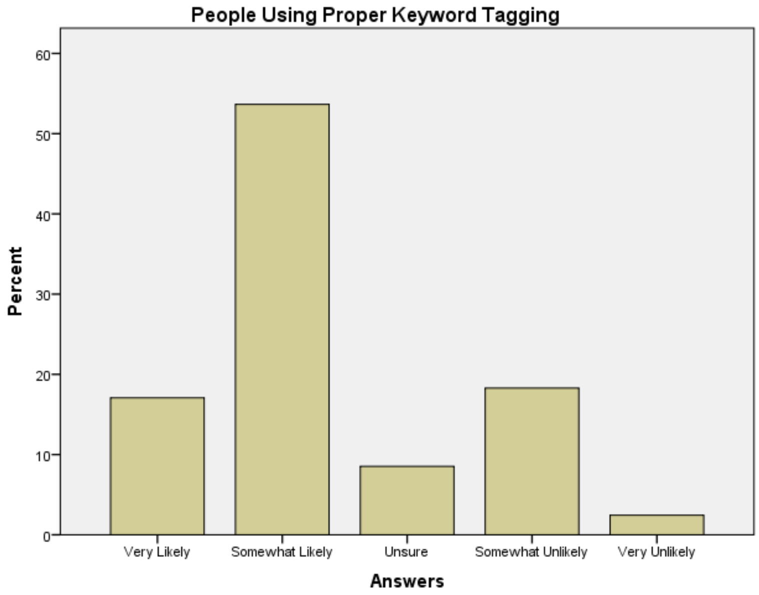

Figure 5 The likelihood of people tagging photos with the relevant keywords in the Keyword Tagging scenario.

In comparing the two fairness questions and the positive response to the question regarding proper keyword use, we conclude that participants believe that they would properly tag photos they upload with the correct keywords. However when it came to photos uploaded by others, they lack the confidence that others would tag photos correctly. This could mean participants are aware of the potential subjectivity in keyword tagging and that ultimately, the major mechanism of this scenario up to each person's individual interpretation of a photo.

The results showed that there was a strong correlation between participants thinking Group Agreement was difficult to use, and participants' fairly negative opinion on the likelihood of unanimous group agreement .047 sig.

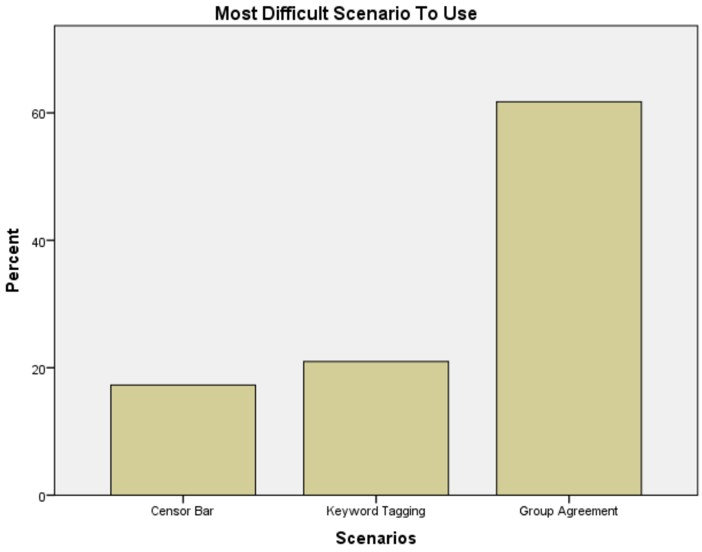

Figure 6 The scenario participants found most difficult to use.

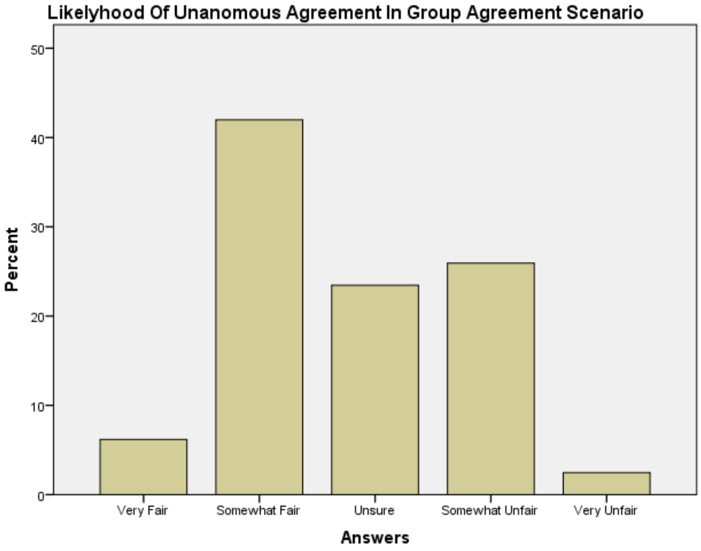

Figure 7 The likelihood of unanimous agreement of a joint privacy policy for a photo in the Group Agreement scenario.

This correlation shows that participants disliked the Group Agreement scenario because they thought it was too cumbersome to get all individuals involved to completely agree on a collective privacy policy for each individual photo. However, there were slightly more positive responses regarding the fairness of unanimous agreement in the Group Agreement Scenario.

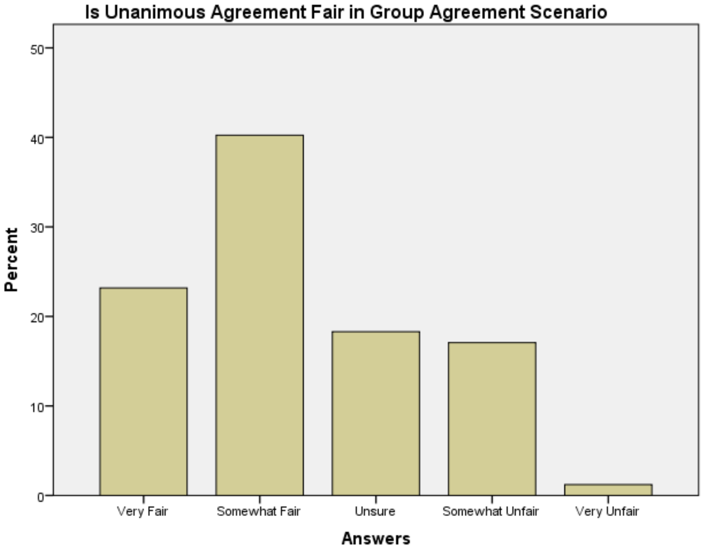

Figure 8 Participants view of the fairness of unanimous agreement in joint privacy policies of photos in the Group Agreement scenario.

This is most likely due to the participants believing the scenario is fair in that everyone involved gets a say in the privacy policy for photos they are tagged in, but despite that, it is impractical for them to use.

Conclusion

In this paper, we have shown that the current state of popular social computing sites is unsatisfactory for the collaborative privacy needs of users. Based on the findings of previous research conducted in the area of individual privacy policy improvement, and on our results pertaining to collaborative privacy scenarios we presented, it is seen that there is a great deal of complexity in each individual users' wants and needs regarding their privacy settings, especially in the area of collaborative privacy management.

The participants of our research preferred the Keyword Tagging collaborative privacy scenario the most in terms of ease of use and when uploading many photo, despite the uncertainty behind incorrect keyword tagging of photos. The least popular scenario was Group Agreement, due to the impractical requirement of unanimous user agreement on the collective privacy scenario for a photo.

Finally, because our research results were not entirely conclusive and there was little correlation between the demographics of participants and their answers regarding the privacy scenarios, a more detailed study with updated collective privacy scenarios could be done, as well as more specific questions regarding why participants liked or disliked specific scenarios could be asked.

References

1. A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tammi. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. Vancouver, BC, Canada, May 2011. CHI.

2. Simon Jones and Eamonn O’Neill. Contextual Dynamics of Group-Based Sharing Decisions. Vancouver, BC, Canada, May 2011. CHI.

3. Andrew Besmer and Heather Richter Lipford. Moving Beyond Untagging: Photo Privacy in a Tagged World. Atlanta, GA, USA, April 2010. CHI.