

Moving Beyond Untagging: Photo Privacy in a Tagged World

Andrew Besmer & Heather Richter Lipford
 Department of Software and Information Systems
 University of North Carolina at Charlotte
 9201 University City Blvd.
 Charlotte, NC 28223
 {arbesmer, Heather.Lipford} @ uncc.edu

ABSTRACT

Photo tagging is a popular feature of many social network sites that allows users to annotate uploaded images with those who are in them, explicitly linking the photo to each person's profile. In this paper, we examine privacy concerns and mechanisms surrounding these tagged images. Using a focus group, we explored the needs and concerns of users, resulting in a set of design considerations for tagged photo privacy. We then designed a privacy enhancing mechanism based on our findings, and validated it using a mixed methods approach. Our results identify the social tensions that tagging generates, and the needs of privacy tools to address the social implications of photo privacy management.

Author Keywords

Privacy, photo sharing, social network sites, Facebook.

ACM Classification Keywords

H.5.m Information Interfaces and Presentation: Miscellaneous

General Terms

Design, Human Factors.

INTRODUCTION

Online photo sharing applications are increasingly popular, offering users new and innovative ways to share photos with a variety of people. Many social network sites are also incorporating photo sharing features, allowing users to very easily upload and post photos for their friends and families. For example, Facebook is the largest photo sharing site on the Internet with 1 billion photos uploaded monthly [8]. Integrating photo sharing within social network sites has also provided the opportunity for user-tagging, annotating and linking images to the identities of the people in them. This feature further increases the opportunities to share photos

among people with established offline relationships and has been largely successful.

Increased access to an individual's photos has led to these images being used for purposes that were not intended. For example, photos on Facebook profiles have been used by employers [13] and law enforcement [15] to investigate the behavior of individuals. User tagging adds a new twist to this problem in that users are often posting photos of other users. As a result, people have reduced control over their image and its reach. This in turn, can lead to greater risks for embarrassment or humiliation over the content of photos. Thus, while users are able to easily share photos and are doing so in incredible numbers, they also need to be able to control their privacy and protect photos from being used against them in some way. While the number of photos being uploaded to Facebook and other sites has continued to increase, privacy controls have remained rather stagnant.

Photo privacy may become even more problematic in the future as researchers are discovering effective automated algorithms to identify people in images and tag them [16]. As facial recognition becomes more accurate, it will be easier than ever before to locate individuals in photo collections and link people between different collections. This makes tagging, and thus sharing, images even easier. Yet this further erodes users' abilities to control the disclosure of their images as they could be automatically identified in many more photos, uploaded by many people.

There has been relatively little research examining the use of photo sharing sites, particularly how that use relates to privacy issues and needs among users. Several studies have examined the social uses and impact of tagging on Flickr, a photo sharing site that does provide some social networking capabilities [4]. Additionally, a number of studies have identified privacy issues related to social networking overall [10, 17]. However, we are not aware of any to date that have examined privacy related specifically to photo sharing in social network sites such as Facebook and MySpace, and the particular privacy problems encountered with photos posted by others.

In this paper, we seek to add to the growing literature by providing a greater understanding of privacy concerns and needs of users, in addition to creating a privacy mechanism

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to publish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA
 Copyright 2010 ACM 978-1-60558-929-9/10/04...\$10.00.

meant to address those needs. To quote the usability mantra, “know thy users” and then design for them. We believe that by first understanding users’ current concerns and behaviors, we can design tools they desire, adopt, and are motivated to use. Other designers will also be able to use our results to do the same.

BACKGROUND

Recent research has started to examine the phenomena of online photo sharing, much focusing on the site Flickr. Flickr not only allows users to upload photos either for private or public consumption, but also promotes annotating to organize related photos. Text labels can be associated with any photo to describe the contents of the image, location, people, or any other property of the photo. While people do create tags to help them organize their photos, they are often used to communicate contextual or social information to those viewing the photo [4]. Thus, online photo activities involve social communication through images with a variety of people.

Privacy issues have also been examined on Flickr. For example, Miller and Edwards found two different cultures of photo users on Flickr [12]. One group shared photos publicly to foster online relationships based around photo discussion. However, most users were primarily concerned with sharing photos of holidays and trips within their existing social circle, and were thus much more concerned with protecting many of these images and keeping them out of public view. Ahern et al. [2] also examined users’ decisions when posting photos to Flickr with mobile camera phones. They found that while some users’ decisions to post privately or publicly were determined by security concerns, many more decisions were made around identity or impression concerns for themselves or others. In both cases, the studies examined users posting their own photos.

Photo sharing is an important component of many general online social network sites. Many researchers have examined how various profile information and social features of these sites are used for managing identity, communicating with social networks, and forming and strengthening relationships [5, 6]. The over disclosures of personal information and potential risks of personally identifiable information on Facebook profiles have also been explored [10]. However, little work has investigated privacy specifically in this domain of photo sharing within social network sites or the issues with photos posted by others. While some aspects may be similar to other online photo sharing, we expect that the large social networks that users tend to build, and the inherent linking of photos to other personal information about users, will lead to different concerns, strategies, and needs regarding privacy management.

In order to better understand privacy problems we must first define what privacy means. There are of course many ways to define what privacy is and how users struggle with it. For this domain, we define privacy as a process of boundary management [3]; individuals alter their behavior to disclose or withhold information in order to manage their iden-

tity and allegiances with others over time [14]. Photo tagging also impacts these boundaries by expanding the audience of users’ pictures in both the present and potentially in the future. Tagging has also enabled users to make decisions about another user’s boundaries by allowing them to attach images to another’s profile. This need not be malicious, a user harmlessly uploading and tagging a photograph of another can have devastating consequences for another user if it conflicts with any of the many social circles to which that user belongs.

Identity and impression management is a familiar problem for users of social networking applications. Many users are beginning to struggle with their professional and personal image as social networking becomes integrated into the workplace [7]. Users struggle with this because they now have so many social circles, some of which overlap, and a single profile in which to share information on. Unfortunately photos, particularly photos that a user is tagged in, have very few privacy controls.

For example, on Facebook, a photo owner creates an album “Friday” which contains photos of himself and several of his friends. As the owner of this album, he can choose which set of his friends can and can’t see this album (by default it is permissive). Tagging another user in any photo in the album attaches that photo to that person’s profile. The tagged user has no privacy controls herself, but can untag herself to remove the explicit reference to the photo on her profile. Optionally, the tagged user can choose to restrict all of her tagged photos from a group of friends, such as hiding them from a workplace. This forces the tagged user to make an all-or-nothing decision with any particular user group. We believe these limited tools have a negative impact on the social value of photo sharing, forcing users to live with socially inappropriate disclosures that they are uncomfortable with. We seek to design additional privacy mechanisms for online photo sharing that fit the social needs of this domain.

UNDERSTANDING THE USERS

In order to better understand our users and the privacy issues in this domain, we held a series of three focus groups in early 2008. We discussed photo sharing, perceptions of user privacy, and current tagging practices for photographs within social network sites. Many questions centered around Facebook because photo sharing on Facebook was familiar to many participants. Participants were recruited by flyers posted on campus and solicitation from undergraduate classes at the university. Our study consisted of three focus groups conducted with 14 total participants. Participants were predominantly female ($n = 8$) and aged 18-24 ($n = 12$) with the remaining participants being 25-39 ($n = 2$). Almost all reported having been a member of Facebook for 1-3 years ($n = 12$) and most logged on more than once a day ($n = 9$).

We first collected demographic information from participants and their use of online photo sharing applications. We then demonstrated the current Facebook photo application and tagging feature. The participants were asked several ques-

tions regarding their use of the photos application, if they ever untagged themselves, and any privacy concerns. After this, we demonstrated a prototype application to blur faces within the tagged photo area to protect an unwanted photograph. We used this as a talking point to get deeper into issues such as ownership, tension, and permanency of decisions. The entire session was recorded for later analysis.

After transcribing each of the focus groups, we analyzed the data using open coding. We coded each focus group for both common and interesting remarks. We then grouped these categories into several overarching issues.

As with other photo sharing sites, users expressed the social value of being able to upload and view photos within their social networks. However, not surprisingly, users do have privacy concerns that are difficult to deal with due to the wide reach of their images and the lack of control over the disclosure of many photos. In discussing privacy issues surrounding photo usage, users expressed a number of general concerns for certain information they do not want to be seen by other people. They also discussed their current mechanisms for coping with these concerns. Throughout the discussions the issue of photo ownership was brought up and is very relevant to the acceptance of our mechanism and other potential privacy mechanisms.

Concerns

We asked participants about their general privacy concerns and any problems they have had when sharing photos. We also asked users about why they untag photos, the current mechanism for removing the link to a particular photo from a profile. These questions revealed a range of concerns about the kinds of information that users do not want revealed to different people. All the reported concerns related to photos that others uploaded.

Users were often keenly aware of specific individuals or groups of individuals who they were concerned of seeing an unwanted photo of them. These concerns were not about the public or strangers viewing their photos, but instead about those who were already within their social circles. Family members such as moms, dads, sisters, and brothers comprised most of the perceived threat. Extended family members and friends were also mentioned as well as employers and organizations to which the participant belonged. Participants had stories about a breach of their privacy by those close to them. For example, P13 described a situation where her sister would let her mother view her profile. She pointed out that *“I’m not doing anything wrong in the pictures; it’s just, you know, she could get me in trouble.”*

We were surprised that in no case did a participant express concern of a stranger finding their photos, and deriving their personal location or personal information from them. This differs from results from previous studies on Flickr, where researchers explored why users chose to disclose images publicly [2]. This also differs from privacy concerns regarding stalking which drives decisions with other profile information on Facebook and other social network sites [17]. Thus,

privacy concerns of tagged users are rarely about security concerns and more about identity and impression management within that user’s social circles.

Incriminating evidence was commonly cited by participants as a concern. The most frequent example participants gave was being intoxicated. For some, the reason was that they were underage and the photograph proves an illegal activity has occurred. One of the older participants talked about how her teenage son *“had a wine bottle last weekend”* in a photograph. She laughingly mentioned that *“he would have loved to delete that picture.”*

However, the activity did not need to be an illegal one. For example, P7, who is a member of a university sports team, reported being tagged in *“a lot of photos”*, and worried about photos of himself being inebriated. P7 says, *“I’m not allowed to be seen in photos on Facebook with alcohol or anything like that because I’m on the [sports] team.”* This reveals the strain with managing his identity, where acceptable behavior among friends and students is not appropriate for members of an organization to disclose. This same tension applies when users want to appear professional to potential employers or others in authority, limiting the desire to disclose photos of certain behaviors.

Another common reason participants indicated they untagged images was unflattering photographs. These photographs portrayed the participant in an unfavorable light. P6 used the example of *“your roommate decided to walk in when you just woke up.”* Several participants seemed to actually expect to be tagged in images where they do not look good. Finally, participants noted that they untagged photos in order to disassociate from people or groups. P5 explains, *“it’s just I don’t wanna be associated... or maybe something happened, we are not friends anymore.”* Thus, users were aware and interested in shaping their identity based upon their associations with different people and groups, and interested in controlling accessibility of certain photos for that reason.

Users expressed a great deal of concern over their lack of control in removing photos from Facebook and from friend’s profiles. While users can untag to remove the explicit reference to them, the photo remains close to them because it is cross-linked to others in the photo and remains accessible from other profiles. This means users are unable to ever completely prevent disclosures of a photo posted by someone else, and that once this photo is there it will never go away. The permanency of a photo being added to the massive collection of photos on Facebook continues to strain user privacy both now and in the future. And users seemed to have a sense that the very people they were concerned about seeing a photograph were actually watching, and would find those photos.

Coping With Concerns

Many participants modified their behavior, both online and offline, to cope with the use and popularity of Facebook photo sharing. First, several users reported frequent un-tagging, P6: *“I spend probably an unhealthy amount of time un-*

tagging pictures on Facebook.” Other users expressed that they do not like to untag because it can offend the person who tagged the photo. Thus, the act of untagging can have negative social consequences and lead users to not protecting their privacy when desired.

Interestingly, tagging was seen to also have some positive privacy benefits by making people aware of the photos that have been posted of them by other people. P8 explains, “*What if it’s pictures out there that you’re not tagged in? How do you know that the picture is out there?*” Tags enable users to review all photos of themselves that exist and some users restrict the entire set of photos. However, this reduces the social value of photo sharing.

Participants reported using a variety of methods outside of Facebook to manage the disclosure and privacy of their photos. Some participants reported using other online sharing methods, such as instant messaging or email which would limit the accessibility of the photos to a smaller group of people. Not only did this protect their own photos, but limited the issues of interfering with friends disclosure boundaries.

Many relied on offline social interaction to handle unwanted images. P2 mentions that “*If I was close enough to the person I would just ask them to remove the photo.*” This obviously relies on the photo owner to honor the person’s request. And, even with close friends, this strategy can still fail. For example, P1 reports that sometimes friends might not agree: “*My friends would be like no, no you look really bad. That’s why it’s of you, we want people to see that, it amuses us.*”

Participants also reported changing their everyday behavior to prevent undesired photos from being taken in the first place. This occurred by trying to stay out of pictures as much as possible and by not behaving in ways that the user would not want recorded in the first place. Despite these strategies, many users expressed their expectation of ending up in photos online that they do not want posted. There was a general hopelessness about this lack of control over images of themselves and acceptance that it was likely to continue to occur. As P6 stated, “*There’s not much you can do about it because it’s someone else’s picture.*”

Ownership

Ownership is an important issue in photos for social network sites, as many users upload photos of other people. We questioned the social acceptance of modifying or deleting photos that perhaps seem to belong to other people. Even before we asked direct questions about ownership or demonstrated our prototype, participants naturally brought up ownership regarding their general concerns and problems of photo sharing. There were two main perceptions participants had regarding ownership of photos. The first, but less widely adopted, opinion is that each individual in the image is a co-owner of that image. The second and more popular opinion is that the person who uploaded the photo remains the owner regardless of those in the image.

Some participants felt that because they were in the image they were also owners of the image and should have the same rights to that image as everyone. Others expressed a general lack of ownership and acknowledged the public nature of posting information on the Internet: “*Once it’s online it’s everybody’s man.*” The group consensus seemed to be that the owner of the photo is the one who uploaded it. This perception is based on the current model of social network sites where the owner has more controls over that image. For example, if someone other than the owner tries to tag the photo, the owner is sent a request to approve that tag. Users also expressed that the person who has the photo has the right to do what they want with it, including post it online, and users were hesitant to take away these rights, even if it violated their own privacy.

However, users also did not want to completely relinquish their own rights for privacy; they still wanted some control over their own image. They expressed that the owner has a “*moral obligation*” to protect the privacy of those in the photo. Thus, users thought owners should behave in a socially appropriate manner to meet the needs of others in the social setting. Yet our participants, when thinking of themselves as owners, did not want others to manipulate the photos they uploaded. This demonstrates the tension between the desires and rights of the owners and the desires and rights of others in the photo, particularly when the owner does not realize or care to act in the interest of others.

This tension can cause complications for future tools if they do not take into account both the photo owner and the individuals within the photo. For example, allowing other users to simply completely remove a photo may not be an acceptable solution as it impinges on the rights of owners to post the photo, and many users would hesitate to use such a feature.

DESIGN CONSIDERATIONS

Our focus groups identified many opportunities for improving user privacy of tagged photos. We realize there is no silver bullet for privacy, but there is room for serious improvement. Our results suggest a number of design considerations or opportunities in this domain:

- **Identity and Impression Management** - Both photo owners and tagged users need to manage their identity and control appearance to different, sometimes overlapping, groups.
- **Social value** - Sharing is usually in the interest of all parties, it is who they want to share with that matters.
- **Monitor Privacy** - Users need to be able to see how far their image reaches across their social network.
- **Known threats** - Users know exactly who they do not want to share with, often those who are close to them. Photo owners may be aware of this as well.
- **Ownership** - Tools need to adhere to general notions of who should own and control the photo.
- **Design around tensions** - Tension between the tagged user and the photo owner exist and can be explicitly included in the design of mechanisms to rely on the social consequences of privacy management.

Restrict others from seeing this photo

To: Bob User

From: Alice User

Regarding: A photo I have been tagged in: 

Please prevent: from seeing this photograph.

[You might also prevent](#)

Optional Reason:

[Suggest Permissions](#) [Cancel](#)

Figure 1. This is an image of the request page for Restrict Others. It allows users tagged in a photo to suggest generic permissions that are negotiated with the owner of the photo.

- **Altruism not guaranteed** - Photo owners are not always socially responsible and sometimes behave in selfish and cruel ways.
- **Immediate action** - Untagging was favorable because it immediately has an impact on the tagged users' ability to manage identity.
- **Communication** - Bring negotiation over photos into privacy mechanisms. Negotiation often occurs offline and could be utilized within a tool.

While some of these considerations are mutually exclusive many of them are not. We used these considerations to design our particular tool. However, many other tools could be created and should keep these considerations in mind.

RESTRICTING OTHERS

We now introduce the “Restrict Others” tool to address photo privacy. It works by allowing tagged users to send a request to the owner asking that a photo be hidden from certain people. The request page is depicted in Figure 1. This tool addresses concerns users have and the short comings of the current mechanisms. It does so in a way that we believe minimally impacts the social value users find in photos and uses naturally existing tensions to help manage user privacy. Restrict Others takes previously out of band communication and integrates it into the management and negotiation of privacy settings between the photo uploader and the tagged user. This mechanism was designed with the following features to address as many design considerations as we could:

- **Identity and Impression Management** - The tagged user is able to set custom permissions at the individual photo level. In addition, individual's names are not passed along in the request to the uploader. Only the number of individuals to be blocked is sent for review.
- **Social value** - Our tool promotes sharing by reducing the need for the tagged user to untag the photo or restrict all their tagged photos. The photo uploader is still free to share the photo with as many or as few people as he or she likes.

- **Known threats** - Our tool lets users specify individuals or groups of users they would like to restrict the photograph from.
- **Ownership** - We still wanted to adhere to the consensus and current model of ownership. Thus, we treat the photo uploader as the owner and allow the co-owner to have a say. The tagged user is not allowed to simply set permissions on the photo since they are not the owner of the photo and this would create tension between the tagged user and the owner. We included elements like who the request was being sent to, who it was from, and the photograph to provide context, and used the word “suggest” in the submit button to convey this model of ownership.
- **Design around tensions** - The request enables the tagged user to exert a tension on the uploader to fulfill the “*moral obligation*” to respect her privacy. Should the owner deny the request the tagged user would be informed of this and be given the option to fall back on untagging the photo. Whatever decision the owner makes will have some sort of an impact on the relationship between the two. In the tagged user's worst case, she would be as protected as she currently is able to be now.
- **Immediate action** - Sending a request temporarily untags the photo during negotiation phase. The tagged user immediately benefits from the additional privacy afforded.
- **Communication** - Restrict Others brings negotiation over the photo explicitly into the social network site in the form of a request.

We implemented our prototype as a Facebook application. Our prototype had access to all of a user's actual photos on Facebook and was designed to very closely resemble the current photos application in terms of look and interaction. When viewing a photo, we inserted a link to “restrict” next to “untag” and a link to “restrict others” within the menu provided by Facebook for each photo. Placement and wording was determined by feedback from our pilot users. We found the words “restrict others” were important as other wording such as “suggest permissions” did not convey an accurate

representation of the mechanism. Using “suggest permissions” as the submit button was acceptable though.

In the design phase we sought to identify possible issues with a mechanism of this sort and address them as much as possible. First, having the tagged user specify who he is concerned about seeing the photograph is problematic in that a blackmail situation might now exist. To mitigate this we decided that names should not be sent in the request but instead the number of people that are to be denied access to the photo. Should the tagged user wish to communicate the actual people or other information to the photo owner, they can do so through the optional reason box. Such reasons may be useful in situations where a large number of people are requested to be blocked.

Currently neither photo owners or tagged users can set permissions on an individual photo. In addition, photo owners are unable to set any settings on the album which involve people they have not added as friends or are not a part of networks they belong to. Our mechanism enables this fine-grained control and allows photo owners to set privacy settings on users which are not within their existing social spheres. In fact, photo owners need not know who they are.

A second problem is this system relies on users recalling each and every user in their social circles which should be denied access. While users do know exactly who they do not want to see the photo it is likely this mental picture is incomplete. For example, if a tagged user was concerned of a church member seeing a photo they are unlikely to recall each and every person in that church. Our implementation included a simple algorithm for determining mutual friends. Researchers are currently working on ways to assist users in identifying other users via clustering [1], tie strength [9], and no doubt many other algorithms based on the social graph. With good algorithms it would be possible for the photo application to proactively inform users when future privacy problems might occur. For example, a tagged user blocks people at their church and later adds a new friend from the church. The photo application can inform the tagged user of a possible privacy problem by pointing out the similarity to the people she previously denied access to the photo.

Evaluation

We used our prototype to develop an in-lab study in which participants would use our software to complete a series of tasks. We recruited our participants through flyers at our university, a local community college, and the Charlotte area in summer 2009. Additionally, participants were recruited through a series of online ad campaigns through the Facebook marketplace and ad system. All participants were offered a small monetary inducement in exchange for their time in our study.

Participants first logged into Facebook and we installed our application to their profile. We then presented participants with a survey in one tab of the browser and the prototype in the other. The survey guided them through the comple-

tion of 3 tasks on Facebook using our prototype. We gave participants no training on the interface and told them that we would restore their settings to be the same as when they arrived upon conclusion of the study.

Tasks 1 and 2 asked participants to select a photo they did not want at least one other person to be able to see and untag or restrict that photograph on Facebook respectively. These tasks were counter-balanced in order to prevent ordering bias. After completing each of these tasks we asked participants to indicate their comfort in performing the task, perceived comfort of the photo’s owner, how much effort the task required, and how protected they felt the photograph now was. We also asked additional questions, for example what action they would take if the request they just sent was denied.

Task 3 instructed participants to continue browsing photos on Facebook until a friend sent them a request. We instructed participants that they should make a decision on that request once it was received. We then injected a fake request using our own photo and labeled the participant as the photo owner. While we had designed the prototype to select a photo from the participant’s album, due to inconsistent results from the Facebook API we were forced to use a photo of our own. The request indicated that there were 6 people a user wished to restrict the photograph from. While Facebook generally allows users to approve, deny, or ignore a request, we removed the option to ignore so they had to make an approve or deny decision.

After approving or denying the request, we asked a similar set of questions as Task 1 and 2. We also asked questions like how reasonable the request was, whether approving the request would impact the usefulness of the photo, and reasons they might deny the request. After this we asked participants demographic information, as well as other general questions about the prototype and untagging.

Results

We had a total of 17 participants with ages ranging 18-59. Participants identified their ages as 18-23 ($n = 12$) and over 26 ($n = 5$). Participants were primarily male ($n = 11$), and self identified as caucasian ($n = 12$). We used Westin’s 2003 privacy segmentation index [11] to classify participants as fundamentalist ($n = 10$), pragmatist ($n = 6$), or privacy unconcerned ($n = 1$). Most reported using the Facebook photos application at least once a week ($n = 14$). Many indicated that they do not have to deal with unwanted photos very often ($n = 12$), with very few indicating they have never had to ($n = 2$). The remaining participants often dealt with unwanted photos ($n = 3$). It is worth taking a moment to note that the study population is predominately college aged students and as a result, some findings may not generalize beyond this group. There may also be both cultural and age related differences that we did not have an opportunity to examine.

We asked participants to report their comfort in performing the task, perceived comfort of the photo’s owner, how much effort the task required, and how protected they felt the pho-

tograph now was using a seven point Likert scale. A score of 1 indicated very little effort, very uncomfortable or unprotected, 4 was neutral, and a score of 7 meant a large amount of effort, very comfortable or protected.

We compared responses to our questions of comfort and effort for Restrict Others and untagging. Table 1 reports the average response to the four questions. It is not our intent to say our mechanism is better than untagging. Restrict Others is a complement to untagging and thus saying one is better than the other is fruitless. However, since untagging is currently the only way tagged users deal with photos, we think that untagging provides the best baseline for us to examine this new mechanism.

After conducting a Wilcoxon signed ranks test we discovered only one of these four aspects were statistically significant. Rather unsurprisingly, participants rated Restrict Others ($m = 2.24, SD = 1.48$) as requiring more effort than untagging ($m = 1.53, SD = 1.07$), $p < .05$. Untagging required only clicking a button while Restrict Others involved defining a friend set.

Table 1. Comparison to Untagging

	Untagging <i>m</i>	Restricting <i>m</i>	<i>p</i>
Self Comfort	5.53	4.65	0.06
Owner Comfort	4.00	4.06	0.74
Protectedness	4.12	4.65	0.16
Effort Required*	1.53	2.24	0.04

*Using Wilcoxon signed ranks test.

Two others trended to differences, but did not achieve significance. Participants indicated they were more comfortable in untagging a photo ($m = 5.53, SD = 1.97$) than they were with Restrict Others ($m = 4.65, SD = 2.23$). In addition, they indicated that Restrict Others ($m = 4.65, SD = 1.53$) resulted in a photo that was more protected than untagging ($m = 4.12, SD = 1.45$). Finally, participants indicated little difference in the photo owners comfort as a result of untagging ($m = 4.00, SD = 1.90$) or using Restrict Others ($m = 4.06, SD = 2.05$).

When presented with a photo request they could approve or deny, participants indicated taking action required little effort ($m = 1.29, SD = .59$). Participants indicated that if they were to approve the request it would not make the photo any more or less useful ($m = 3.94, SD = 1.03$). The majority of participants chose to approve the request ($n = 14$) and found it to be a reasonable request ($m = 6.14, SD = 1.29$). Those that denied the request ($n = 3$) found the request to be somewhat unreasonable ($m = 3.00, SD = 1.732$). We later discuss reasons why.

We found that approving the request ($m = 5.00, SD = 2.51$) and denying the request ($m = 5.00, SD = 2.64$) had similar levels of self reported comfort. However, there was a difference in how comfortable the tagged user would be as a result of their action. Participants perceived that approving a request ($m = 5.57, SD = 2.174$) would result

in the tagged user being more comfortable than denying the request ($m = 3.00, SD = 1.00$).

Unpacking Results

To better understand what lies behind these numbers we asked participants several open-ended questions. Their responses help us better understand what is occurring. We begin by looking at why it may be more uncomfortable to send a request than to untag. Sending a request requires negotiation with another person while untagging requires no interaction with the photo's owner. The only way for a photo owner to know about the action is for them to re-look at the picture and notice someone is no longer tagged. Some might also feel uncomfortable because they perceive sending a request is an admission of guilt, P13 says: *"It feels like I'm trying to hide something, but at the same time... I am."* While it is more uncomfortable than untagging, it is not likely to be any more uncomfortable than calling the person on the phone or sending them an email to make such a request. Discomfort may also be a result of novelty and lack of experience using the tool, but we have no evidence to indicate how much.

We saw little difference in the perceived comfort of the photo owner when participants thought of themselves as the tagged user. P9: *"... it conveys a message to a friend who uploaded the picture that I did not like it. So next time he can keep it in mind."* Other participants mentioned that it did not feel like they were making a strong request only a *"simple suggestion"*. This is also consistent with the previous notions regarding the photo owners' moral obligation to the tagged user.

From the point of view of a tagged user, there is no perceived change in comfort for the photo owner. However, our quantitative and qualitative analysis indicate when actually asked to protect another user's privacy, a tension is exerted on the photo owner. Many participants indicated that they could not see a reason they would not approve the request of another. One participant even said it would be *"pretty ridiculous to deny the request for any reason"*, another said that *"it would be obnoxious not to"*. Many of the responses talked about the rights of the person in the photograph, the cause of their moral obligation. However, we still see that there are times, as we previously feared, that a person would not care to act on the behalf of others.

We reviewed cases where the participant denied the request and identified reasons for their doing so. Some of the reasons the participant mentioned included no reason being supplied by the tagged user, the photograph not being controversial, the owner not being in the photo, and having never seen the requesting user before. Therefore, the photo owner will still likely rationalize about the appropriateness of the request and the impact on themselves. When the photo owner has little interest in protecting others the request will not be approved. This seems more likely when the tagged user has little or no existing relationship with the photo owner. In cases like these, the tagged user could fall back on untagging.

In choosing who to block a photo from, participants most commonly requested that a member of their family ($n = 7$) be blocked from seeing a photograph. School friends ($n = 6$) and work ($n = 5$) were also very commonly requested to be blocked from seeing a photograph. At times these overlapped. The remaining groups were made up of roommates, church, specific friends, and so on. No one attempted using a predefined friends list, although we supported that ability.

While some participants expressed that they could not recall everyone, only one used the feature for suggesting similar friends to block. We asked participants why they did not use the button and the overwhelming response was that they did not notice the feature. This may be a feature that needs to be better integrated into the task either through automatically populating a list or prompting after submission. A few participants indicated they would have rather been presented with pictures of their friends to choose from instead of manually entering them. We were afraid, that given the average number of friends (120), this might be too overwhelming. The friend suggestions did use pictures for up to 20 friends.

All of our participants seemed to understand how Restrict Others worked without being given an explanation. Most viewed Restrict Others in a very positive light. P5 says: *“I like the fact that once it’s done, it is extremely unlikely that it will be undone, whereas untagging may be easily undone.”* It is not uncommon for untagged users to become retagged, either accidentally or intentionally. Provided their request is accepted, being tagged is no longer an issue. In our focus groups, we found users might appreciate having been tagged in a bad photo. The tag alerts them to the presence of the photograph in the social network. As such, photos that remain tagged with our mechanism will keep users informed of who can and can’t see the photograph. In addition, it would be possible as we previously described to proactively manage privacy as new friends enter the user’s social graph.

Only two participants reported not liking Restrict Others. Both of their reasons were rejection of the ownership idea altogether. P5 said: *“I don’t think their profile management is my business.”*, and *“Ultimately however, I’m not ‘in charge’ of the dissemination of the photograph, thus untagging or suggestion permissions is a moot point.”* So while the mechanism appeals to those with the more popular view of ownership, it still does not address the needs of other views.

We asked generally of all users what about Restrict Others they disliked. While many indicated there was nothing they disliked, others disliked the restrict only nature of settings, inability to remember every person, and notions of ownership. Because of the nature of this mechanism we saw many cases where participants felt they did not want to have to ask another person to confirm the settings. These would be similar to people in our first study who saw themselves as co-owners. For example, P17: *“I feel that I should be able to block my friends from seeing the photo without asking permission of someone else.”* or P9: *“I would like to have the rights to make the setting. And he just needs to be informed about it.”*

DISCUSSION

Our exploration of photo sharing on social network sites reveals that this domain does have unique privacy needs due to the widespread sharing of images and the social implications of user tagging. In work by Ahern et al. [2], users who were deciding whether or not to upload photos did consider the social implications, such as how their actions influence others’ online identity, and the convenience of sharing. In uploading a photo, the owner has made a decision that the photo should be shared and can determine who it should be shared with.

Ahern et al. also point out that even when given the choice of a public vs. private album, users will sometimes choose public to ensure the person they intend to share it with is able to view the photo. Tagging on Facebook facilitates this social sharing by assisting owners with ensuring that those in the photo get access to it by explicitly permitting those who are tagged. Such permissive default privacy mechanisms make sense for a lot of reasons. Social network sites benefit from increased interaction and page visits over the uploading and viewing of content. Each user also benefits from the social value of sharing, learning, and interacting around photos.

However, current privacy mechanisms on social network sites put the photo uploader, the owner, in control of determining the reach of the photo. Tagged users are not afforded the same controls. For example, on Facebook, the uploader of the photo has the ability to restrict the entire album through privacy settings. Yet the tagged user can only restrict their entire set of tagged photos, or remove the tag on a particular photo. Restrict Others seeks to allow each party to utilize maximum social value while minimizing the overexposure of a photograph for each of the users in it.

For tagged users, identity and impression management is the driving force behind their privacy concerns. They want to better control their image and its reach and currently have a very limited ability to do so. Yet this means that multiple people desire control over a photo, resulting in this ownership tension we have discussed throughout the paper. Shared control leads to conflict and the need to determine who decides on the outcome and what that outcome should be. The differing notions of ownership described by our participants in both studies reflect where they believe control resides in this domain: with owners, with tagged users, or some combination. Whatever tools people use, the parties must resolve the conflict using any one of many strategies. Social negotiation is one possibility, competition another. Any access control or privacy mechanisms for such shared media will have social implications and require users to do conflict reduction in some way.

For example, researchers have identified five different conflict strategies: competing, collaborating, compromising, avoiding and accommodating [18]. The untagging mechanism on Facebook can result in competing over tagging and untagging. The photo owner is able to tag a photo, the tagged user untags it, and the owner retags it, creating the competition cycle. This cycle will continue until one party forfeits, and

unfortunately for the tagged user still results in protections they are likely less than comfortable with. Despite the childish sounding nature of this competition, several of our focus group participants reported this very behavior. Users are also currently using other conflict strategies such as avoiding by altering their behavior in the physical world to stay out of photos.

Our new mechanism, while simple, attempted to manipulate the ownership tensions involved by providing a collaborative tool in a way that benefited all parties. A collaboration strategy was identified as having many long term benefits such as satisfaction, trust, and affection. Collaboration is also the most assertive and cooperative method [18]. Our goal in the Restrict Others mechanism was to explicitly deal with and manipulate the ownership tension and need for conflict reduction. Being on the receiving end of a request to restrict certain people resulted in social tension exerted on the photo owner to honor that request. It appears that in most cases our mechanism will work and owners will feel that obligation to respect another's request. This is because the satisfaction, trust, and affection of friends, among other things, is impacted by the decision the owner makes. This also explains why in cases where little or no established relationship exists our mechanism might be prone to failure. The owner then has little at stake regarding his decision. In cases like these users may wish to use other strategies that are less cooperative, and may need additional tools to do so.

The downside to using such a collaborative mechanism, of course, is that photo owners might at times feel bothered by requests or fail to deal with them, reducing the effectiveness of the mechanism. Similarly, tagged users sometimes felt they should not need to first get approval from an owner for protection to be provided. One possible change which seems promising based on our qualitative feedback is to allow tagged users to change the settings and notify the owner. The owner can then explicitly deny the setting and prevent future changes by that person if they disagree, but the default is allow. This might lessen the burden on photo owners while still allowing them to be in control and retain the traditional notion of ownership. Additionally, tagged users may in turn feel more in control over photos of them because their actions provide immediate privacy benefits. Additional study would be needed to determine the best balance and variations of collaborative control on different sites, as well as to determine if our findings extend to a wider demographic. Additionally, our results may be specific to the United States; notions of ownership are likely impacted by culture and country. Thus, different tools may be more acceptable in different cultures.

While Restrict Others was a tool which was highly understood, needed, and accepted by our participants, it is not the only tool that is needed. Users do want more tools to help them manage their privacy in photo collections on social network sites that we did not address. All users need more awareness and control of the disclosures of photos. For example, photo owners still need fine-grained access control for individual photos within an album. Tagged users still

need tools to use in situations where little trust or benefit is offered to owners for collaboration. These tools will likely adopt different strategies of compromise, competition or collaboration. Explorations of these additional privacy tools need to be grounded in a solid understanding of the social implications of the ownership tensions and conflicts.

CONCLUSION

Photo sharing on social network sites has grown tremendously to over a billion new photos a month. Yet the tagging of photos on social network sites such as Facebook has caused users to lose control over their identity and information disclosures. Users have very few controls to manage socially appropriate photo sharing across their many overlapping social spheres. Users are forced to accept the resulting problems because of a strong desire to participate in photo sharing.

Our findings reveal a number of important design considerations for photo privacy tools around the importance of identity and impression management and the tensions of ownership. Restrict Others explicitly dealt with the natural tension that arises between the owner of the photo, and those tagged in it. We created a lightweight means for users to negotiate desired sharing, complementing the existing privacy coping mechanisms that users currently employ. In manipulating these ownership tensions, we believe our tool would help users achieve more desired privacy while still maximizing the social value of sharing.

While this study focused on Facebook in particular, other social network sites such as MySpace also support user tagging in photos. The concerns and issues we discovered will likely be applicable to this and other general social network sites with photo sharing. As these sites continue to grow in popularity and users add more and more photos, meeting users' privacy needs is important to allow safe and comfortable participation on these online communities. We continue to investigate privacy concerns and new mechanisms to improve privacy management in online social networking communities.

REFERENCES

1. F. Adu-Oppong, C. K. Gardiner, A. Kapadia, and P. P. Tsang. Social circles: Tackling privacy in social networks. July 2008. Poster presented at SOUPS 2008.
2. S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair. Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 357–366, San Jose, California, USA, 2007. ACM.
3. I. Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Pub. Co, Monterey, Calif, 1975.
4. M. Ames and M. Naaman. Why we tag: Motivations for annotation in mobile and online media. In *Proceedings of the SIGCHI conference on Human*

- factors in computing systems*, pages 971–980, San Jose, California, USA, 2007. ACM.
5. danah michele boyd. Friendster and publicly articulated social networking. In *CHI '04 extended abstracts on Human factors in computing systems*, pages 1279–1282, Vienna, Austria, 2004. ACM.
 6. danah michele boyd and J. Heer. Profiles as conversation: Networked identity performance on friendster. In *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 3, page 59c, 2006.
 7. J. M. DiMicco and D. R. Millen. Identity management: Multiple presentations of self in Facebook. In *Proceedings of the 2007 international ACM conference on Supporting group work*, pages 383–386, Sanibel Island, Florida, USA, 2007. ACM.
 8. Facebook. Statistics. <http://www.facebook.com/press/info.php?statistics>, 2009.
 9. E. Gilbert and K. Karahalios. Predicting tie strength with social media. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 211–220, Boston, MA, USA, 2009. ACM.
 10. R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80, Alexandria, VA, USA, 2005. ACM.
 11. P. Kumaraguru and L. F. Cranor. Privacy indexes: A survey of westins studies. *Institute for Software Research International*, 2005.
 12. A. D. Miller and W. K. Edwards. Give and take: A study of consumer photo-sharing culture and practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 347–356, San Jose, California, USA, 2007. ACM.
 13. J. Palank. Face it: Book no secret to employers - The Washington Post, July 2006.
 14. L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, Ft. Lauderdale, Florida, USA, 2003. ACM.
 15. A. Romano. Walking a new beat: Surfing MySpace.com helps cops crack the case. - Newsweek, Apr. 2006.
 16. Z. Stone, T. Zickler, and T. Darrell. Autotagging facebook: Social network context improves photo annotation. In *Computer Vision and Pattern Recognition Workshops, 2008. CVPRW '08. IEEE Computer Society Conference on*, pages 1–8, 2008.
 17. K. Strater and H. R. Lipford. Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1*, pages 111–119, Liverpool, United Kingdom, 2008. British Computer Society.
 18. K. W. Thomas. Conflict and conflict management: Reflections and update. *Journal of Organizational Behavior*, 13(3):265–274, May 1992.