Privacy Decisions for Location-Tagged Media

Shane Ahern, Nathan Good, Simon King, Mor Naaman, Rahul Nair
Yahoo! Research Berkeley
1950 University Avenue, Suite #200
Berkeley, CA, USA

{sahern, ngood, simonk, mor, rnair}@yahoo-inc.com

ABSTRACT

We studied privacy decisions made by users in a system that recorded contextual information (e.g. location, tags, and time) for photos taken with mobile phones. We looked at data from a 3-month long deployment, and conducted interviews with six of the users. We found that content is key when users make photo privacy decisions, and that for some users, the photo location serves as a good predictor for privacy preferences. As for location disclosure, zip-code level disclosure was not a significant issue for most users.

Categories and Subject Descriptors

H.4.M [**Information Systems Applications**]: Miscellaneous

General Terms

Human Factors, Experimentation, Privacy

Keywords

Privacy, location privacy, location-aware, camera phone

1. INTRODUCTION

Location-aware ubiquitous computing applications expose users to a new set of privacy concerns [3]. These concerns are amplified when location is tied with photographs because, over time, a collection of location-tagged photos shows not only a history of the locations frequented by a user, but may also disclose the user's relationship to the location: e.g., home, school, office. ZoneTag [1] is a photo upload application for camera-phones that automatically associates photos with location data (in zip code granularity). The photos are saved to Flickr [2], a photo sharing website, and the location information is displayed on Flickr as textual tags.

Flickr, and thus ZoneTag, support two basic privacy modes: public (discoverable and viewable to any visitor to the Flickr website) and private (visible only to the photo owner, or extended to Flickr users the owner designates as 'friends' or 'family'). For the purpose of this study, we do not make the distinction between different types of 'private' photos. Users can change the privacy settings for each photo they upload. By default, ZoneTag keeps the privacy settings from one photo to the next.

In this work, we examine ZoneTag user behavior in managing privacy of location-tagged photos through user interviews and descriptive analysis of the ZoneTag dataset. We first generally describe privacy patterns as they relate to user activity in the system. Then, we analyze "location-based privacy", or patterns in which users apply different privacy settings. These patterns can show us whether, as one user phrased it, "some locations are more private than others". Finally, we consider "privacy of location": the issue of location disclosure as exposed in our system.

2. STUDY

Over three months, we collected data for over 120 users who have uploaded at least ten images to Flickr using ZoneTag, and conducted formal interviews with a six ZoneTag users.

Overall, more private photos (59%) were uploaded than public (41%). Of our users, 16% had exclusively private photos, while 24% had exclusively public photos. For the 60% users who had a mix of photos, 55% of these were private, and 45% were public.

2.1 Patterns of Privacy

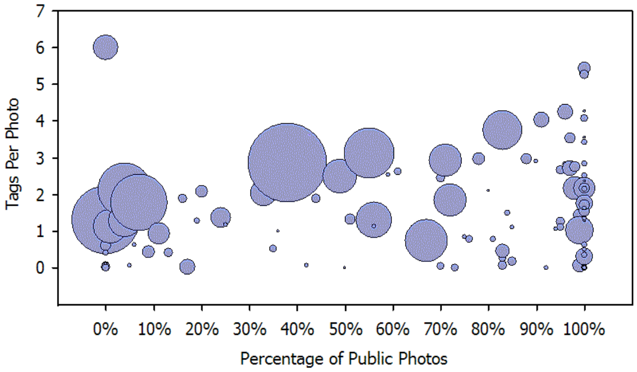
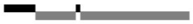


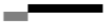
Figure 1: The number of tags per photo vs. the percentage of public photos for each user.

Figure 1 depicts the set of ZoneTag users according to the percentage of public photos in their account. Each user is represented by a circle; the circle area is proportional the number of photos taken by the user. The Y-axis represents the average number of textual tags added by the user to their photos. Users with a higher proportion of public photos tend to use more tags for each photo. For example, "all-private" users (left side of the figure) averaged 1.2 tags per photo, and "all-public" (right) averaged 1.9 tags per photo. We suspect this correlation is due to the fact that public photos are primarily intended for sharing on Flickr, and additional tags make photos more discoverable on the Flickr website. Figure 1 also suggests that users who are more familiar with the system (i.e., have taken more photos) are more likely to change privacy settings (leading to the large circles near the middle of Figure 1).

We observed several patterns in per-user privacy changes over time. We list each of these patterns, and illustrate them using the inline figures, below[1]. Each figure shows a representative user's privacy history in which time moves from left to right; public photos appear as thin black bars above the midline, and private photos appear in gray, below the midline.

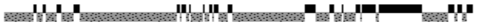
[1] Using Sparklines (http://sparkline.org/)

Public changed to private.  Some users started taking exclusively public photos, and then switched to mostly private photos. When one user saw the vast quantity of publicly viewable photos on Flickr, and the personal nature of the content of many of those photos, he remarked: “I ended up being more sensitive [about photos being public] than I thought I was”. After this realization, the user decided to make all his photos private.

Private changed to public.  Other users started uploading photos privately, and then changed to primarily public photos. In our interview, subjects suggested that the switch was for the purpose of sharing. One user mentioned that they sent links to their photos via email “all the time, [to] everyone I work with, 100-150 people…[I sent it] directly to them.” In this case, the photos needed to be public for others to access them.

All Public or All Private. Some users decided to keep all photos public or private.

In the three classes of privacy patterns mentioned above, convenience seems to play a large factor. User interviews did not reveal a connection between the user’s mental model in making these decisions and the location where the photos were taken, or the fact that location data about the photos was exposed.

Mixed Settings.  Many users alternated more rapidly between private and public photos. One user said that she based her privacy decisions on both the content and the location of the photo. If she felt the photo was potentially embarrassing she made it private. Or if the photo was taken in her home or in the home of friends or family members, she tended to make it private. Another user made all photos of family members private, but any other photos public. “If it’s a family [photo] or the kids, then I’d like it private”.

Tag data from our users confirmed this mental model. We have looked at tags that appear in our (internal) users’ data. We found that many of the tags that appear primarily on private photos tend to describe family members, and are often related to home.

2.2 Context of Privacy

Previous work [3,4] describes location as an important factor in privacy. To examine the relationship between location and privacy in the context of photo collections, we looked at how individual users make their photo privacy decisions in different locations. We calculated the ratio of public photos to private photos for each user in each location (zip code). Then, locations for each user were grouped according to their deviance from the overall public/private ratio for the user. The result is shown in Figure 2. We show three classes of locations for each user: locations where the user is more likely to make photos public (bottom bars, green), locations where the local public/private ratio matches the overall norm (middle, yellow), and locations where a user is more likely than usual to make photos private (top, red). The location-sensitivity of users’ privacy decisions clearly varies. Some users (left side of Figure 2) make similar decisions everywhere they take photos. Others show a acute shift in privacy preferences based on the location (right side). The users we interviewed seem to confirm this. One user stated “I don’t worry about people knowing where I was [when I took a photo]. If I was worried about that, I wouldn’t take pictures [that reveal my location]”. Another user made all pictures he took in his home private: “I wouldn’t want people to rob me. [If they] saw a picture of my stuff and knew where I lived I’d be nervous.” Again, looking at tags (from internal users) that appear mostly in private and not in public photos, we noticed many that are location-specific like users’ homes, a gym, a work place etc.

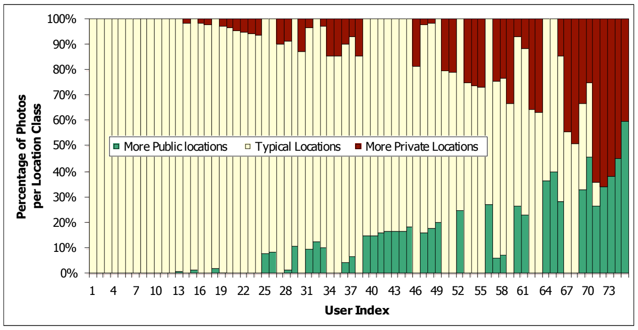


Figure 2: Percentage of photos taken in each location class, by each user.

2.3 Other Observations

During the study, we did not encounter many user concerns about disclosure of location to an institutional third party (e.g. government). It appears that most users’ concerns regarding photo privacy were centered around exposing their photos publicly.

The granularity at which the users expect the location data to be exposed may have an effect on the privacy and location disclosure decisions. We found that different users are comfortable with different levels of location granularity. One user commented that “city information is okay, but I’m not sure about zip codes”, while another user had no problem with exposing the zip code even for his home, but was averse to exposing the exact coordinates.

3. CONCLUSION

User privacy concerns seemed especially sensitive to the content, and often to the location of the photograph. Users seem to manage these concerns both through the adjustment of public/private settings when taking photos, and through choosing the types of photos that they take. Sharing these photos exposed additional complications, as users are forced into awkward compromises between public and private in order to easily and effectively share photos with other users. Location disclosure at Zip code granularity did not seem to be a significant issue for most users.

This study represents a preliminary exploration of questions around mobile photos and location information, and interesting future directions to pursue. We would like to compare location-disclosing decisions to simple photo-sharing decisions, as well as examine in more detail the contextual factors that may contribute to users’ decisions on making photos public or private.

Location-based photo services are becoming exceedingly popular on the web. These services could serve as a benchmark for ubiquitous computing applications where users “leave a mark” regarding their actions and whereabouts (e.g., [5]). This study provides a first view at users’ expectations and behavior in such systems.

4. REFERENCES

[1] ZoneTag. http://zonetag.research.yahoo.com

[2] Flickr. http://flickr.com

[3] Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In Proc. of CHI '05, ACM Press (2005), 81--90.

[4] R. Hull, B. Kumar, D. Lieuwen, P. F. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas, "Enabling Context - Aware and Privacy-Conscious User Data Sharing," MDM 2004..

[5] Plazes. http://www.plazes.com