A Survey on Privacy Recommendation for Images on Social Network

Kshitij S. Ahirrao[1], Aditi Jahangirdar[2]

[1]Department of Information Technology, MIT College of Engineering, Pune, India

[2]Professor, Department of Information Technology, MIT College of Engineering, Pune, India

Abstract: ***Now-a-days people share many personal images on social network which requires maintaining privacy. Privacy is required to prevent the misuse of such images. For keeping these images secure various privacy settings are required. If a tool is provided to the user which will make him set privacy easily, this will reduce his task. For addressing this need several techniques are proposed. In this paper some privacy recommendation techniques are discussed. These techniques recommend privacy to user for images. For recommending such privacy, user profile information and properties of images are used. Tags related to images and visual properties also important to classify images.***

Keywords: social network, image privacy, privacy recommendation

1. Introduction

Images are now useful for user's connectivity. Sharing of images takes place within group of known people or social circle and increasingly outside the group, for discovery of new people. Some images might be content sensitive. Sharing images on content sharing sites may lead to unwanted disclosure and privacy violations[1]. Persistence nature of media gives rich aggregated information about the owner of content and subject of content[2]. The collected information can results in unexpected exposure of one's social environment and lead to misuse of one's personal information.

Most social networking and content sharing sites provide set privacy preferences. Unfortunately, user finds difficult to set privacy and maintain it[3]. The large amount of shared information makes process error prone and tedious. Therefore there is need of policy recommendation system which can be useful for user to easily and properly configure the privacy setting[4].

In this paper, several techniques are summarized which provides hassle free privacy setting mechanism. These techniques handle factors which influence privacy setting and user uploaded images:

- *The impact of social environment and personal characteristics.[5]* Social context of user, such as user's profile information and his groups of social network may be useful for knowing about user's privacy preferences. For example, student may not wish to share his college photographs with family members. However, using common policies for all users or similar users may not satisfy individual's preferences. Users may have different opinions for same type of image. For example someone may be willing to share all his images but conservative person may not. Therefore we have to find balancing point between impact of social environment and personal characteristics. Moreover, person may change their opinion about particular type of images. In order to develop personalized system, such changes in user's behavior should be considered carefully.
- *The role of image's content and metadata.[5]* In general, similar images often incur similar privacy preferences. For example, one may upload several photos of family members and specify that only family members are allowed to see those pictures. He may upload some other photos of landscapes as hobby and he may set privacy preference such as allow everyone to view.

Analyzing the visual content may not be sufficient to predict user's privacy preferences. Tags and other things give social context of images, including where and why it was taken and also provide other description about image.

Rest of the paper divided into following section.

Section II includes methods proposed for privacy recommendation for images on social network. Section III comprises of the summary of paper.

2. Methods Proposed For Privacy Recommendation For Images On Social Network

A. Privacy suites[6]

Bonneau et al. [6] proposed the concept of privacy suites which recommends users a set of privacy settings that "expert" users or other trusted friends have already set, so that users can either directly choose a setting or only need to do minor modification.

In proposed technique there are four building blocks. The first building block is an Abstract Specification Format for privacy settings. It splits the privacy specification from UI to enable modifying of sophisticated setting. Experts can define a Privacy Suite via privacy programming in this block as follows:

```
def showPhotoStream(self, user):
 if user in self.friends: return True
```

```
mutualFriends = self.friends.intersection(
 user.friends)
if len(mutualFriends) > 10: return True
else: return False
```

Distribution must be done after privacy suite is created. This could be done via existing channel, or through the social network. Users can adopt a suit which is used by a trusted friend. Each user can post link on their profile indicating which privacy suite they are using.

After importing a suite and customizing it, a key challenge for a user is to map his friends into the roles that are used by the suite for role-based access control decisions (e.g. identifying friends, family members or co-workers). If designed poorly, this process could be as difficult as managing privacy settings under the current UI. Thus, main requirement is to have an effective interface that can quickly assign friends and groups of friends into roles designed by a newly adopted suite. This could be initially seeded by placing friends into groups based on the social circle they are in. A user could then graphically handle these groups, dragging them into the necessary roles and overriding them as needed.

A system for applying privacy suites should have a mechanism to update user's settings because of continuous change in environment. If user does not trust the author's suite to perform automatic updates; he could choose to adopt a suite "statically". If he chooses "dynamically", he will automatically receive the owner's changes as new features are introduced.

Maintenance might become difficult if users have excessively customized a suite. Simple local changes such as blocking a specific individual may conflict with updates.

B. Social circle finder[7]

Adu-Oppong et al. [7] develop privacy settings based on a concept of "Social Circles" which consist of clusters of friends formed by partitioning friend lists.

Users of social-networking sites share huge amount of personal information with a large number of "friends". Social networking sites have recognized the need for privacy mechanisms that allow users to control friends to see selected information. Grouping several hundred friends into different lists, however, can be a laborious process.

To alleviate the burden of categorizing a large number of users into meaningful lists, authors propose a technique called Social Circles Finder for generating these lists automatically. The clusters of densely and closely connected friends, or social circle can be viewed as uniform groups from the perspective of privacy settings. Social circle finder provides following features.

Social-graph visualization

Visualize the social circles of users by rendering such as shown in Fig. 1. It would help users make more well-informed and hence better decisions about their privacy settings.

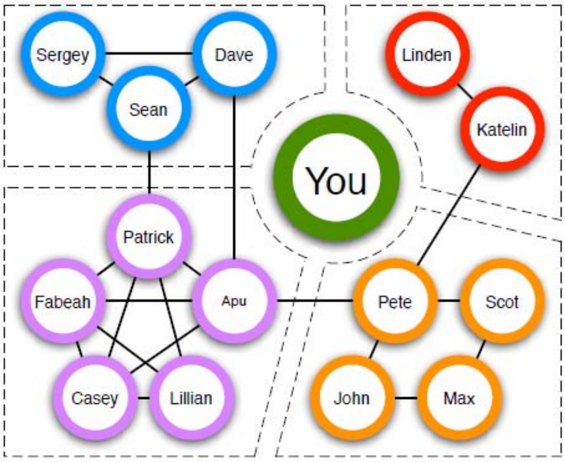


Figure 1: Visualization of social circle [7]

Privacy-settings recommendation

On the basis of identified social circles, recommend set of friend lists user should create and the friend lists into which they should put each of their current friends.

Social Circles Finder would be able to, with proper integration into the Facebook platform, provide the above features not just when users are browsing their friends, but also when they are adding new friends.

Social circles are meaningful from a privacy point of view and thus Social Circles Finder is effective, if the user tend to choose to share the same combination of personal information with friends in the same social circle but different combinations with friends in different social circles.

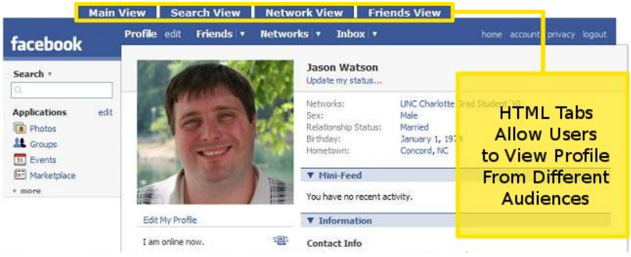
C. Audience view[8]

Heather et al.[8] proposed to structure the privacy setting interface as the information that a particular audience (other users)- search, network, friend, or self- can see.

Authors were examining the role of interface usability in current privacy settings and preparing Report on iterative prototype, where presenting an audience oriented view of profile information significantly improved the understanding of privacy settings.

This will help the user associate privacy settings with how their information is presented to different people group instead of the lists of privacy menus. This interface is a series of tabbed pages, where each page presents a separate audience view of a profile, along with controls for showing or hiding information to that group. Thus, the interface provides visual feedback as to the effect of modifying privacy settings, along with an accurate model of information to be shared.

Authors are currently iteratively prototyping their proposed interface. In first iteration, the audience view is created and examined without any mechanism for modifying settings, similar to Orkut's interface. This allows verifying that this visual feedback is useful and provides guidance for continued design. The prototype, shown in Fig. 2 and Fig. 3, adds a set of tabs for each audience.



Jason Watson

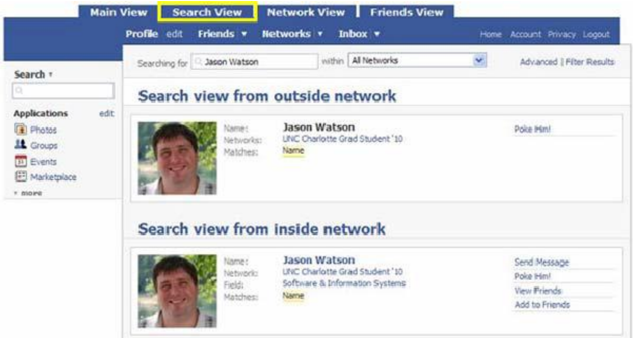
Networks: UNC Charlotte Grad Student '10
Sex: Male
Relationship Status: Married
Birthday: January 1, 197
Hometown: Concord, NC

You have no recent activity.

I am online now.

HTML Tabs Allow Users to View Profile From Different Audiences

Figure 2: Added view tabs[22]



Searching for Jason Watson within All Networks

Search view from outside network

Name: Jason Watson
Networks: UNC Charlotte Grad Student '10
Matches: Name

Search view from inside network

Name: Jason Watson
Network: UNC Charlotte Grad Student '10
Field: Software & Information Systems
Matches: Name

Figure 3: Search view tab [8]

D. Tag and linked data[9]

Authors in [9] have presented an expressive language for images uploaded in social sites. While photo sharing sites provide tools for setting up an online album, users who want to maintain a certain level of privacy are usually provided with primary access control only. Given that descriptive tags are greatly used on photos, and that the Semantic Web provides a common means of sharing social network information as linked data. Better access control mechanism can be provided by combining the two. Based on this idea, authors proposed a system which allows users to create expressive access control policies for their photos on the Web by using both tags and linked data.

This system depends on the OpenID protocol for authentication, extends the Tag Ontology to represent tagging activities in a photo album, uses the AIR (AMORD in RDF) Policy Language to specify access control policies, and uses the Tabulator as the basis of the user interface for browsing photos (and their metadata in RDF [Resource Description Framework]) and specifying access control policies.

Semantic Web and Linked Data

The Semantic Web provides a framework which describes data on the Web with machine-readable metadata. It also encourages linked data, the idea of connecting data on the Web by using their dereferenceable URIs.

Different roles of a user becomes more clearly defined in the Semantic Web, therefore access control schemes which uses linked data will find it simpler to determine whether the user is authorized to perform a particular task.

Ontologies of tagging

Assigning descriptive keyword to online resources such as images is known as tagging. Several ontologies have been developed to conceptualize tagging and allow reuse of tagging.

The OpenID Authentication protocol

It is an authentication protocol which gives users a single digital identity that can be used to log on to different Web sites. A user chooses a trusted OpenID provider with which he maintains a unique ID in the form of an URL to use OpenID. Other systems will depend on this OpenID provider to authenticate user. The FOAF (Friend Of A Friend) ontology provides the property foaf:openeid for specifying the OpenID of a foaf:Person. If user is the person mentioned in FOAF profile then he can be verified, thus provides a decentralized authentication method for semantic web application.

The AIR Policy Language

AIR (AMORD in RDF) is a policy language which is represented in RDF and gives several classes and properties for defining policies. An advantage of using AIR is that the reasoner will return explanation of why access to certain photos is compliant with the policies.

The Justification UI extension of Tabulator can be used to provide a clear presentation of the explanation. This helps user to review his policies and verify if rules are properly defined.

Tabulator

The Tabulator consists of both a browser and an editor of RDF data on the Web. It allows a user to check out data related to a particular resource on the Web by automatically recognizing and following RDF links. It also allows user to modify RDF data in the same interface. Tabulator is chosen in this project because of several of its features like; Tabulator can be easily extended to give a customized view of data of a particular type, while the user can still travel through the RDF data using the standard views. In addition, Tabulator provides mechanisms for updating the RDF data if it detects that the data sources is modifiable.

System design

The main component of proposed system is the server side script (Fig. 4) which mediates interactions between the user, the RDF data storage and external services such as OpenID providers and the AIR Reasoner.

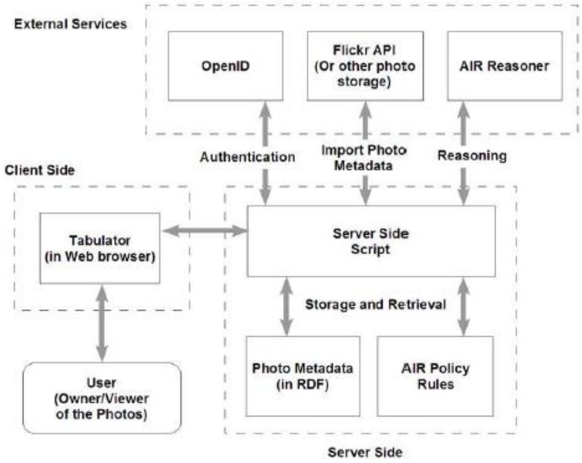


Figure 4: System architecture for tag and linked data based system [9]

The system allows user to login using their FOAF URI. The user can create and modify his photo albums, and providing an interface in tabulator to import metadata of photos from host Web site. User can create new access control policies for own photo albums and also browse the photo album of other users. In this case the server side script will collect all relevant data, including the FOAF profile of the owner, the photo album RDF data and the access control policies, and provide them to the AIR Reasoner which determines whether the user is authenticate to access the photos. The server side script will then serve RDF data to the user based on the result of the reasoner.

E. PViz[10]

User's mental models of privacy and visibility in social networks generally involve subgroups, or communities, within their networks of friends. Such groupings are not always clear and existing policy comprehension tools are not naturally aligned with this mental model. Authors introduced PViz, an interface and system which corresponds more directly with the way user's model groups and privacy policies applied to their social networks. PViz allows the user to understand the visibility of her profile according to natural sub-groupings of friends, and at different levels of granularity.

The PViz policy comprehension tool shows the user's social network which is centered on a graphical display. Each node in the display represents sub-group of the user's friends (a community) or an individual friend. To the left of the graphical display, PViz shows a list of profile items for which the user can configure and set privacy settings. To view privacy settings for a specific item, the user must choose the item from the list. To show privacy settings in PViz the user can see the color of the node (i.e., subgroup) which ranges from 0% (light) to 100% (dark) and is given based on the user's privacy selection for a selected profile item. Alternatively, placing the mouse over a node opens an explicit numerical popup.

PViz also includes the potential to view communities, subgroups and privacy settings at different levels of granularity by zooming in and out. In addition to the graphical display, PViz provides many ways of communicating with the social network graph to improving exploration. User can search for a friend's name in a search box and display will automatically center on the node containing that friend. A text box displays the names of all members of the currently selected node (community).

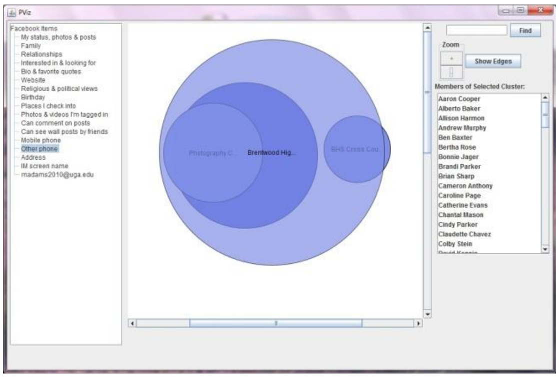


Figure 5: GUI of PViz[10]

F. Adaptive Privacy Policy Prediction(A3P)[5]

Authors proposed an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. Role of social context, image content, and metadata as possible indicators of user's privacy preferences is examined. The proposed system in this paper has a two-level framework which determines the best available privacy policy for the user's images being uploaded according to the user's available history. Solution depends on an image classification framework for image categories. Policy prediction algorithm will automatically generate a policy for each newly uploaded image, also according to users' social features. Over time, policies will follow user's privacy attitude.

A3P system is comprised of two main building blocks (as shown in Fig. 6): A3P-Social and A3P-Core. The A3P-core focuses on examining each individual user's own images and metadata, while the A3P-Social offers a community view of privacy setting recommendations for a user's potential privacy improvement. Authors designed the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

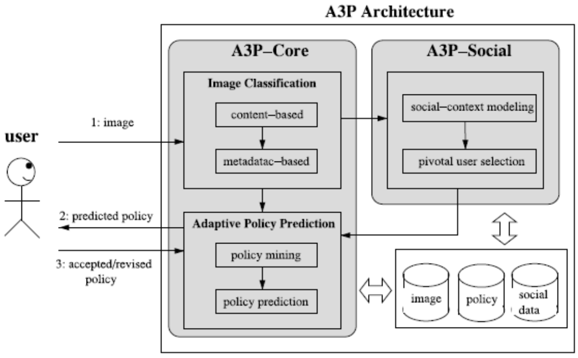


Figure 6: Adaptive Privacy Policy Prediction (A3P) framework[5]

When a user uploads an image, the image will be sent to the A3P-core. The A3P-core categorizes the image and determines whether there is a need to invoke the A3P-social. In most cases, on their historical behavior A3P-core predicts policies for the users. If one of the following two cases is verified correct, A3P-core will invoke A3P-social:

1) The user does not have sufficient data for the type of the uploaded image to conduct policy prediction;
2) The A3P-core detects the recent large amount of changes among the user's community about their privacy practices along with user's increase of social networking activities (new friends added, new posts on profile etc.).

In above cases, it would be favorable to report to the user the latest privacy practice of social communities that have similar background as the user. The A3P-social assembles users into social communities with similar social context and privacy preferences, and continuously observes the social groups. When the A3P-social is invoked, it identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be sent to the user for display.

If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can select to revise the policy. The actual policy will be stored in the policy repository of the system for the policy prediction for images get upload in future.

3. Summary

Tremendous amount of data is shared on social networking. Most of the time this data consists of images. All this kind of data requires privacy to protect from misuse. But many times applying privacy on data become difficult because of tedious and lengthy process. In this paper, different methods are studied which make privacy setting easier for user. User's social environment and characteristics, and image's content and its metadata are useful to predict privacy policy for user. Using all this content and above methods privacy recommendation can be easier.

References

[1] 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 Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.

[2] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in Proc. ACMSIGCOMMConf. Internet Meas. Conf., 2011, pp. 61–70.

[3] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming," in Proc. 5th Symp. Usable Privacy Security, 2009.

[4] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable PrivacySecurity, 2009.

[5] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha Sundareswaran, and Joshua Wede "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE transactions on knowledge and data engineering, vol. 27, no. 1, january 2015

[6] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Sharedprivacy for social networks," in Proc. Symp. Usable Privacy Security,2009.

[7] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008.

[8] H. Lipford, A. Besm r, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.

[9] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

[10] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.