Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Survey on Privacy Policy Specification System for User Uploaded Images Over Popular Content Sharing Sites

Miss. Minal R Hirulkar[1], Prof. Vinod Gangwani[2]
[1]Student of M.E, Department of Computer Science and Engineering, H.V.P.M.'s C.O.E.T., Amravati, India
[2]Assistant Professor, Department of Information Technology, HVPM's College of Engineering & Technology , Amravati.

Abstract: ***The regular use of social networking websites and application encompasses the collection and retention of personal and very often sensitive information about users. This information needs to remain private and each social network owns a privacy policy that describes in-depth how user's information is managed and published. As there is increasing use of images for sharing through social sites, maintaining privacy has become a major problem. In light of these incidents, the need of tools to aid users control access to their shared content is necessary. This problem can be proposed by using an Privacy Policy Prediction system to help users compose privacy settings for their shared images. To examine the indicators of users privacy preferences one can use the role of social context, image content, and metadata as possible according to information available. Our solution relies on a two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded. We propose a two-level image classification framework to obtain image categories which may be associated with similar policies. Then, we develop a policy prediction algorithm to automatically generate a policy for each newly uploaded image. This will generate policies that will follow the evolution of user's privacy according to his requirement.***

Keywords: ***Adaptive Privacy Policy Prediction (A3P), Policy Mining, web-based services***

I. INTRODUCTION

Social media's become one of the most crucial part of our daily life as it enables us to communicate with a lot of people. With the extensive use of digital cameras and the increase of content sharing websites (eg. Flickr, Picasa, etc.) people can now easily publish their photos or videos online and share them with family, friends, coworkers, etc. While extremely convenient, this new level of pervasiveness introduces acute privacy issues. semantically rich images may reveal content sensitive information. Consider a photo of a students 2011 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students BApos family members and other friends.

Revealing personal content on social networking services can expose sensitive information about users. These services typically allow users to create connections to 'friends' such that this content can be shared amongst them and restricted from the wider public. However, these connections rarely distinguish between different types of relationship. Even within a network of 'friends', users may wish to manage the sharing of information and content with different people based on their differing relationships.

Tools for maintaining privacy settings in social media frequently couple control (specifying who can access what) with awareness and comprehension (understanding who can access what, given the existing configuration). However, existing tools do not necessarily account for the types of "queries" users would like to make to reconcile their mental models of the system state (or desired state) with the policy defaults of the system, the limitations of the system's privacy management features, and individually-enacted settings.

Sharing images within online content sharing sites, therefore, may quickly lead to unwanted revelation and privacy violations. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and preserve such privacy settings [1], [2], [3]. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone.

Therefore, many have acknowledged the need of policy recommendation systems which can help users to easily and properly configure privacy settings [4], [3], [5], [6]. However, existing proposals for automating privacy settings appear to be insufficient to address the unique privacy needs of images, due to the amount of information implicitly carried within images, and their

relationship with the online environment wherein they are exposed. Recommender systems can be defined as programs which attempt to recommend the most suitable privacy policy to particular users by predicting a user's interest in an content based on related information about the image. The aim of developing recommender systems is to reduce information overload by retrieving the most relevant information and services from a huge amount of data, thereby providing personalized services. The most important feature of a recommender system is its ability to "guess" a user's preferences and interests by analyzing the behavior of this user and/or the behavior of other users to generate personalized recommendations.

An Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images:

The impact of social environment and personal characteristic. Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. For example, users interested in photography may like to share their photos with other amateur photographers. Users who have several family members among their social contacts may share with them pictures related to family events. However, using common policies across all users or across users with similar traits may be too simplistic and not satisfy individual preferences. Users may have drastically different opinions even on the same type of images. For example, a privacy adverse person may be willing to share all his personal images while a more conservative person may just want to share personal images with his family members. In light of these considerations, it is important to find the balancing point between the impact of social environment and users' individual characteristics in order to predict the policies that match each individual's needs. Moreover, individuals may change their overall attitude toward privacy as time passes. In order to develop a personalized policy recommendation system, such changes on privacy opinions should be carefully considered.

The role of image's content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos. He may upload some other photos of landscapes which he took as a hobby and for these photos, he may set privacy preference allowing anyone to view and comment the photos. Analyzing the visual content may not be sufficient to capture users' privacy preferences. Tags and other metadata are indicative of the social context of the image, including where it was taken and why, and also provide a synthetic description of images, complementing the information obtained from visual content analysis.

II. LITERATURE REVIEW AND RELATED WORK

Bonneau et al. [7] proposed the concept of privacy suites which recommend to users a suite of privacy settings that "expert" users or other trusted friends have already set, so that normal users can either directly choose a setting or only need to do minor modification. Adu-Oppong et al. [8] develop privacy settings based on a concept of "Social Circles" which consist of clusters of friends formed by partitioning users' friend lists. Ravichandran et al. [6] studied how to predict a user's privacy preferences or location-based data (i.e., share her location or not) based on location and time of day. Fang et al. [5] proposed a privacy wizard to help users grant privileges to their friends. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to construct a classifier which classifies friends based on their profiles and automatically assign privacy labels to the unlabeled friends. More recently, Klemperer et al. [9] studied whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access-control policies.

The aforementioned approaches focus on deriving policy settings for only traits, so they mainly consider social context such as one's friend list. While interesting, they may not be sufficient to address challenges brought by image files for which privacy may vary substantially not just because of social context but also due to the actual image content. As far as images, authors in [10] have presented an expressive language for images uploaded in social sites.

Social networking services present many advantages for information dissemination and interpersonal communication, but the copresence of multiple social groups from different facets of a user's life can present a significant challenge for controlling privacy and online identity. Many users experience a perceived loss of control over their personal information and content when using online social networking services [11].

Default privacy settings on services such as Facebook are often configured such that content is shared uniformly with all of a user's contacts. Achieving fine-grained control is an arduous process, yet people consider such control important for presenting multiple versions of themselves [12] or for minimizing the appearance of characteristics that are contrary to an idealized version of themselves [13]. Ackerman and Mainwaring [14] emphasize that, while valued, privacy is not the users' primary task and making it an explicit task for the user can be problematic. Designing privacy management tools that do not require significant configuration

effort from the user is therefore an important and worthwhile objective. Systems that automate, recommend or assist with privacy management decisions could reduce the burden placed on users while providing satisfactory levels of control.

Gross and Aquisti study privacy settings in a large set of Facebook users, and identify privacy implications and possible risks. Lange [18] studies user behavior with respect to revealing personal information in video sharing. All of these papers point out lack of user awareness regarding exposure of aggregated contextual information arising from users' resource sharing habits.

There is a plethora of work dealing with the problem of establishing suitable access policies and mechanisms in social Web environments. Caminati and Ferrari [19], for example, propose collaborative privacy policies as well as techniques for enforcing these policies using cryptographic protocols and certificates. Felt and Evans [20] suggest to limit access to parts of the social graph and to certain user attributes. Squicciarini et al. [21] introduce privacy mechanisms in social web environments where the resources might be owned by several users. In [22], the authors discuss the problem of defining fine-grained access control policies based on tags and linked data. The user can, for instance, create a policy to specify that photos annotated with specific tags like "party" can only be accessed by the friends specified in the user's Friend of a Friend (FOAF) profile.

Vyas et al. [23] utilize social annotations (i.e. tags) to predict privacy preferences of individual users and automatically derive personalized policies for shared content. These policies are derived based on a semantic analysis of tags, similarity of users in groups, and a manually defined privacy profile of the user. Ahern et al. [24] study the effectiveness of tags as well as location information for predicting privacy settings of photos. To this end, tags are manually classified into several categories such as Person, Location, Place, Object, Event, and Activity.

Analysis of visual and textual image (meta-)data is applied to tackle a variety of problems, such as determining attractiveness [25] or quality [27] of photos, search result diversification [28], and others. Figueiredo et al. [26] analyze the quality of textual features available in Web 2.0 systems and their usefulness for classification.

III. EXISTING SYSTEM

Chen et al. [15] proposed a system named SheepDog to automatically insert photos into appropriate groups and recommend suitable tags for users on Flickr. They adopt concept detection to predict relevant concepts (tags) of a photo. Choudhury et al. [16] proposed a recommendation framework to connect image content with communities in online social media. They characterize images through three types of features: visual features, user generated text tags, and social interaction, from which they recommend the most likely groups for a given image. Similarly, Yu et al. [17] proposed an automated recommendation system for a user's images to suggest suitable photo-sharing groups.

Anna Squicciarini developed an Adaptive Privacy Policy Prediction (A3P) system, a free privacy settings system by automatically generating personalized policies. The A3P handles user uploaded images based on the person's personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. The disadvantage of A3P is inaccurate privacy policy generation in case of the absence of meta data information about the images. Also A3P has manual creation of meta data log data information that leads to inaccurate classification and also violation privacy.

IV. ANALYSIS OF PROBLEM

Sharing images within online content sharing sites, therefore, may quickly lead to unwanted revelation and privacy violations.

Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content.

The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

Access rights (such as view only, download and expiration date) is not provided or used.

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. PROPOSED WORK

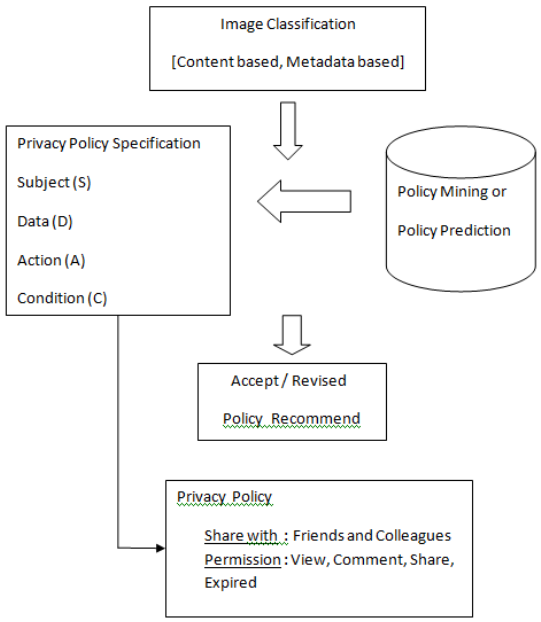

Fig 1.Proposed Work

The proposed method is outlined in fig 1. image classification

To obtain groups of images that may be associated with identical privacy preferences, we propose a hierarchical image classification which classifies images first based on their contents and then separate each category into subcategories based on their metadata.

Policy Mining or Policy Prediction Policy mining is carried out within the same category of the new image because images in the same category are more likely under the identical level of privacy protection.

The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user rivacy Policy Specification

Users can express their privacy preferences about their content revelation preferences with their socially connected users via privacy policies. We define privacy policies according to Definition.

Definition**.** A privacy policy P of user u consists of the following components:

Subject (S): A set of users socially connected to u.

Data (D): A set of data items shared by u.

Action (A): A set of actions granted by u to S on D.

Condition (C): A boolean expression which must be satisfied in order to perform the granted actions.

Accept / Revised Policy Recommend

At the end, the predicted policy will be displayed to the user. If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can choose to revise the policy. The actual policy will be stored in the policy depository of the system for the policy prediction of future uploads.

VI. CONCLUSION

This system will be useful in social sites while image upload, automatic policy generation can be demonstrated, on social sites, while commenting/posting policy changes can be made in real time. An Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. This system also assists Excellent Privacy Preference finding facility, Policy Recommendation System, Easy to use, Excellent security policies, Modify/accept privacy policies.

REFERENCES

[1] Acquisti and R. Gross, “Imagined communities: Awareness, information sharing, and privacy on the facebook,” in Proc.6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[2] 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.
[3] H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability,Psychol., Security, 2008.
[4] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security,2009.
[5] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.
[6] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
[7] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security,2009
[8] 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.
[9] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, and M. Reiter, "Tag, you can see it!: Using tags for access control in photo sharing," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 377–386.
[10] 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.
[11] Hewitt, A. and Forte, A. (2006), Crossing boundaries: Identity management and student/faculty relationships on the Facebook, Proc. CSCW06. ACM.
[12] DiMicco, J. M. and Millen, D. R. (2007). Identity management: multiple presentations of self in facebook. Proc. GROUP '07. ACM, 383-386.
[13] Goffman, E. (1959). The Presentation of Self in Everyday Life. New York: Doubleday.
[14] Ackerman, M. and Mainwaring, S. (2005). Privacy Issues in Human-Computer Interaction. In L. Cranor and S. Garfinkel (Eds.), Security and Usability: Designing Secure Systems that People Can Use, 381-400, Sebastopol, CA, O'Reilly.
[15] H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu,and J.-LWu,"Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning," in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.
[16] M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D. Seligmann, "Connecting content to community in social media via image content, user tags and user communication," in Proc.IEEE Int. Conf. Multimedia Expo, 2009, pp.1238–1241.
[17] J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1464–1467.
[18] P. G. Lange. Publicly private and privately public: Social networking on youtube. JCMC'08.
[19] B. Carminati and E. Ferrari. Privacy-aware collaborative access control in web-based social networks. In LCNS Springer(2008), 5094, 81-96.
[20] A. Felt and D. Evans. Privacy protection for social networking platforms. In Web 2.0 SP'08.
[21] A. Squicciarini, Mohamed, and F. Paci. Collective privacy management in social networks. In WWW'09
[22] C. M. Au Yeung, N. Gibbins, and N. Shadbolt. Providing access control to online photo albums based on tags and linked data. In SSW'09.
[23] N. Vyas, A. Squicciarini, C. Chang, and D. Yao. Towards automatic privacy management in web 2.0 with semantic analysis on annotations. In CollCom'09.
[24] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, and R. Nair. Over-exposed?:privacy patterns and considerations in online and mobile photo sharing. In CHI'07.
[25] J. San Pedro and S. Siersdorfer. Ranking and classifying attractiveness of photos in folksonomies. In WWW '09.
[26] F. Figueiredo, F. Bel´em, H. Pinto, J. Almeida, M. Gonc¸alves, D. Fernandes, E. Moura, and M. Cristo. Evidence of quality of textual features on the web 2.0. In CIKM'09.
[27] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung. Personalized photograph ranking and selection system. In MM '10, New York,USA, 2010.
[28] R. Leuken, L. Garcia, X. Olivares, and R. Zwol. Visual diversification of image search results. In WWW'09.