International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

A Survey On Privacy Policy Inference for Social Images

Miss. Chaitrali A. Salunke

Student, Computer Engineering Department, V.P College of Engineering, Baramati, Maharashtra, India

---

Abstract - ***Social media has become one of the ultimate important parts of our daily life as it enables us to communicate with a many people. Creation of social networking sites such as Facebook LinkedIn etc, individuals are given opportunities to meet new friends in their own and also in the other variety of communities across the world. So that many of the photo sharing applications or content sharing applications on these sites allow users to annotate photos with those who are in them. A number of researchers have studied the social uses and privacy issues of online photo sharing or content sharing sites , but less have explored the privacy issues of photo sharing in social networks. Users of social-networking services share abundant information with numerous "friends." This improved technology causes to privacy violation where the users are sharing the enormous volumes of images across more number of peoples. This privacy need to be taken care in order to make better the user satisfaction level. Towards or focusing on this need, using Adaptive Privacy Policy Prediction (A3P) system to assist users compose privacy settings for their images. Our main contribution to the existing work is to generate user profile, further the privacy inference policies should be mainatained with respect to user profile.***

Key Words: *Social media; content sharing.*

1. INTRODUCTION

Creating privacy controls for social media or networks that are both expressive and usable is a major challenge. The word "social media" refers to the outspread of Internet-based and mobile services that allow users to participate in online exchanges, bring user-created content, or join online communities. Online social networks or sharing/content sites are websites that allow users to build or construct connections and relationships to other Internet users. Social networks store information remotely, rather than on a user's personal computer. Social networking can be used to keep in touch with friends, make new friends and find people with similar interests and ideas. The relation between privacy and a person's social network is multi-faceted. So it required to develop more security mechanisms for different communication technologies, especially online social networks. Privacy is very important to the design of security mechanisms. Most social networks providers have provide an opportunity of privacy settings to allow or refuse others access to personal information details. In certain event or an occasion we want information about ourselves to be known only by a small circle of close friends, and not by strangers or unknown people. In other side, we are willing to reveal our personal information to strangers, but not to those who know us better. Social network theorists have studied the relevance of relations of different depth and strength in a person's social network and the valued of so-called weak ties in the flow of information across different nodes in a network. An Internet privacy can be define as the ability to control what information one reveals about oneself, and who can access that information. Essentially, when the data is gathered or analyzed without the knowledge or permission of its owner, privacy is violated. When it comes to the usage of the data, the owner should be informed about the purposes and aim for which the data is being or will be used. Most content sharing or photo sharing websites permit users to enter their privacy preferences.

Unfortunately, recent studies have shown that users struggle or it is difficult to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tiresome and error-prone. Therefore, many have recognized the need of policy recommendation systems which can help users to easily and properly configure privacy settings. However, existing system for automating privacy settings appear to be insufficient to address the unique privacy needs of images due to the amount of information absolutely carried within images and their relationship with the online environment wherein they are exposed. The privacy of user data can be given by using two methods.

1. The user can enter the privacy preferences

2. Usage of recommendation systems which helps users for setting the privacy preferences.

The privacy policy of user uploaded data can be provided depends on the user social environment and personal characteristics. Social context of users, such as their profile information and relationships with others may provide beneficial information regarding users' privacy preferences. The privacy policy for image which is uploaded by user can be provided depend on the user uploaded image's content and its metadata. A hierarchical image classification which classifies images first based on their contents and then decides each category into subcategories based on their metadata. Images that do not have metadata will be classed together only by content. Such a hierarchical classification provides by A3P system which gives a higher priority to image content and reduces the influence of missing tags[1].

2. LITERATURE SURVEY

Many studies and analysis have been performed on privacy policy techniques.

Alessandra Mazzia et al. [2012] introduced PViz Comprehension Tool , an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks. It allows the user to understand the Visibility of her profile according to automatically natural sub-groupings of people. Because the user must be able to identify and differentiated automatically-constructed groups, we also address the important sub-problem of producing effective group labels. PViz tool is better than other current policy comprehension tools Facebook's Audience View and Custom Settings page.

Peter F. Klemperer et al. [2012] developed a tag based access control of data shared in the social media sites. A system that generates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the user's friends. The participants can select a suitable preference and access the information. Photo tags can be divided as organizational or communicative based on the user needs. There are several important limitations to our study design. First, our results are limited by the participants we recruited and the photos they provided. A second set of disadvantages concerns our use of machine generated access-control rules. The algorithm has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. As a result, some rules appeared strange to the participants, potentially driving them toward explicit policy-based tags like "private" and "public.

Sergej Zerr et al. [2012] proposed a technique Privacy-Aware Image Classification and Search to automatically detect private images, and to enable privacy-oriented image search. It combines textual meta data images with variety of visual features to give security policies. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects that can indicate the presence or absence of particular objects (SIFT). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.

Choudhury et al. [2009] 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, an automated recommendation system for a user's images to provide suitable photo-sharing groups.

Jonathan Anderson et al. [2009] proposed Privacy Suites which allows users to easily choose "suites" of privacy settings. A privacy suite can be created by an expert using privacy programming. The privacy suite is distributed through distribution channels to the members of the social sites. The drawback of a rich programming language is less understandability for end users. Given a sufficiently high-level language and good coding practice, motivated users should be able to verify a Privacy Suite. The main goal is transparency, which is essential for convincing influential users that it is safe to use.

Ching-man Au Yeung et al. [2009] proposed a access control system based on a decentralised authentication protocol, descriptive tags and linked data of social networks in the Semantic Web. It allows users to create expressive policies for their photos stored in one or more photo sharing sites, and users can specify access control rules based on open linked data provided by other parties.

Danezis et al. [2009] proposed a machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced. It develop privacy settings based on a concept of "Social Circles" which consist of clusters of friends. User's privacy preferences for location-based data based on location and time of day.

Fabeah Adu-Oppong et al. [2008] developed concept of social circles. It provides a web based solution to protect personal information. The technique named Social Circles Finder, which automatically generates the friend's list. It is a technique that analyses the social circle of a person and identifies the intensity of relationship and therefore social circles obtained a meaningful categorization of friends for setting privacy policies. The application will identify the social circles of the subject but not show them to the subject. The subject will then be asked questions about

their willingness to share a piece of their personal information. Based on the answers the application finds the visual graph of users.

Kambiz Ghazinour et al. [2008] designed a recommender system known as Your Privacy Protector that understands the social net behavior of their privacy settings and recommending privacy options. It uses user's personal profile, User's interests and User's privacy settings on photo albums as parameters and on the basis of these parameters the system constructs the personal profile of the user. It automatically learned for a given profile of users and assign the privacy options. It allows users to see their current privacy settings on their social network profile, namely Facebook, and detects the possible privacy risks. Based on the risks it adopts the necessary privacy settings.

Fang et al. [2007] proposed a privacy wizard to assist 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 divides friends based on their profiles and automatically assign privacy labels to the unlabeled friends.

3. CONCLUSIONS

This paper describes various privacy policy techniques for user uploaded images in various content sharing sites. The privacy policy can be applied based on the user social behavior and the user uploaded image content. Privacy policy techniques among the existing systems. Future research leads towards improving the performance by a novel semantic retrieval of images.

REFERENCES

1. Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha Sundareswaran, and Joshua Wede, "Privacy Policy Inference of User- Uploaded Images on Content Sharing Sites" IEEE Transaction On Knowledge And Data Enginnering, VOL. 27, NO. 1, January 2015 193

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

3. 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.

4. S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search," in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44.

5. H. Sundaram, L. Xie, M. De Choudhury, Y. Lin, and A. Natsev, "Multimedia semantics: Interactions between content andcommunity," Proc. IEEE, vol. 100, no. 9, pp. 2737–2758, Sep. 2012.

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

7. 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.

8. J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining.,2009, pp.249–254.

9. 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.