Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 6, June -2016

Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites

SURVEY PAPER

Ms.Sayali P.Patil[1], Assistant Prof. Madhuri Zawar[2], H.O.D. & Associate Prof. Dipak Paradhi[3]

[1,2,3]Computer Engineering. Godavari College of Engg & Tech, Jalgaon, sayali9760@gmail.com

Abstract — *In this paper Social media's become one of the most important part of our daily life as it enables us to communicate with a lot of people. Creation of social networking sites such as MySpace, LinkedIn, and Facebook, individuals are given opportunities to meet new people and friends in their own and also in the other diverse communities across the world. Users of social-networking services share an abundance of personal information with a large number of "friends." This improved technology leads to privacy violation where the users are sharing the large volumes of images across more number of peoples. This privacy need to be taken care in order to improve the user satisfaction level. The goal of this survey is to provide a comprehensive review of various privacy policy approaches to improve the security of information shared in the social media sites.*

Keywords *— Social media; Content sharing sites; Privacy; Meta data*

I. INTRODUCTION

The online social networking sites are the websites that enable users to join online communities, make new contacts, find old friends, and share common interests and ideas with large number of people across the world. It allows us to communicate with other internet users and build connections. The kinds and numbers of these content sharing sites have grown and participation of users also increased. As part of their participation lot amount of personal information are shared. Particularly young internet users share private images about themselves, their friends and classmates without being aware of the consequences. Photo sharing users often lack awareness of privacy issues. Many photos publicly shared by young people are of such a private nature that they would not show these images to their parents and teachers. A variety of risks are faced by individuals, such as identify theft, stalking, embarrassment, and blackmail as a result of proliferation of personal data .Despite these risks, many privacy mechanisms of content sharing sites are very weak.

There is a need to develop more security features in online social networks. Privacy is critical feature among the security mechanisms. In some situations, we like to share information only to best friends, family members and in other instances we like to share with strangers also. Existing sharing platforms do not support users in making adequate privacy decisions in multimedia resource sharing. On the contrary, these platforms quite often employ rather lax default configurations, and mostly require users to manually decide on privacy settings for each single resource. Given the amount of shared information this process can be tedious and error-prone [1].

To address the unique privacy needs of images existing proposals for automating privacy settings are inadequate. A definition of internet privacy is it involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large scale computer sharing. The privacy of user data can be given in two ways. 1. The user can enter the privacy preferences alone 2.Usage of recommendation systems which assist users for setting the privacy preferences.

The privacy policy of user uploaded data can be provided based on the personal characteristics. The privacy preferences of a user can be obtained from their profile information and relationships with others. The privacy policy of user uploaded image can be provided based on the content and Meta data of user uploaded images. A hierarchical classification of images gives a higher priority to image content.

Which allows users to easily choose "suites" of privacy settings? A privacy suite can be created by an expert using privacy programming. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. The privacy suite is distributed through existing distribution channels to the members of the social sites. The disadvantage 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 [2].

It provides a web based solution to protect personal information. The technique named Social Circles Finder 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 provide 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 [3].

The social net behavior of their privacy settings and recommending reasonable privacy options. It uses user's personal profile, User's interests and User's privacy settings on photo albums as parameters and with the help of these parameters the system constructs the personal profile of the user. It automatically learned for a given profile of users and assigns the privacy options. It allows users to see their current privacy settings on their social network profile, namely face book, and monitors and detects the possible privacy risks. Based on the risks it adopts the necessary privacy settings [4].

An interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks. PViz allows the user to understand the visibility of her profile according to automatically-constructed, natural sub-groupings of friends, and at different levels of granularity. Because the user must be able to identify and distinguish automatically-constructed groups, we also address the important sub-problem of producing effective group labels. PViz is better than other current policy comprehension tools Face book's Audience View and Custom Settings page [5].

A system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends. The participants can select a suitable preference and access the information. Photo tags can be categorized 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 limitations 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 or arbitrary to the participants, potentially driving them toward explicit policy-based tags like "private" and "public [6].

The impact of social environment and personal characteristics. 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.

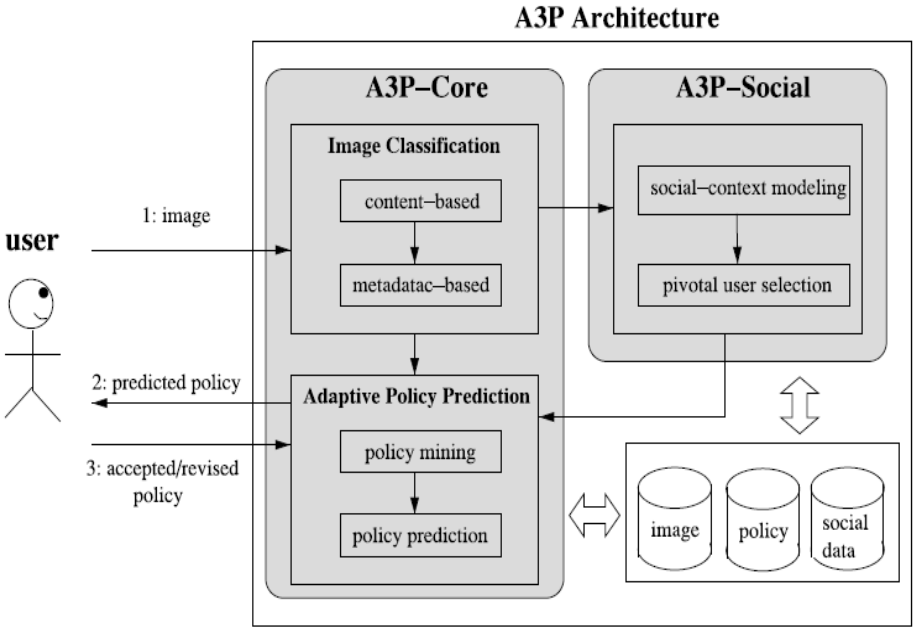

Figure 1: System Overview

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.

Corresponding to the aforementioned two criteria, the proposed A3P system is comprised of two main building blocks (as shown in Fig. 1): A3P-Social and A3P-Core. The A3P-core focuses on analyzing each individual user's own images and metadata, while the A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. We design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice. To assess the practical value of our approach, we built a system prototype and performed an extensive experimental evaluation. We collected and tested over 5,500 real policies generated by more than 160 users. Our experimental results demonstrate both efficiency and high prediction accuracy of our system. A preliminary discussion of the A3P-core was presented. In this work, we present an overhauled version of A3P, which includes an extended policy prediction.

Algorithm in A3P-core (that is now parameterized based on user groups and also factors in possible outliers), and a new A3P-social module that develops the notion of social context to refine and extend the prediction power of our system. We also conduct additional experiments with a new data set collecting over 1,400 images and corresponding policies, and we extend our analysis of the empirical results to unveil more insights of our system's performance.

II. PRIVACY CONCERNS WITH SOCIAL NETWORKING SITES

Privacy concerns with social networking services is a subset of data privacy, involving the binding personal privacy concerning storing, re-purposing, provision to third parties, and displaying of information through the Internet. Each day these sites process large amount of information. In order to gain access of other user's private information features like messages, invitations, photos, open platform application other applications are helpful. In the case of Facebook privacy features are weak .Various level of privacy are offered by these sites. There are even sites in which user doesn't reveal their actual names. It is also possible for users to block other users. Most users do not realize that while they may make use of the security features on Facebook the default setting is restored after each update.

The privacy strategies introduced by our participants may have initially achieved desired privacy protection and matched their initial mental models of audience and accessibility, but these strategies often failed now due to excessive use. When making decisions regarding the disclosure of information and privacy, users who are new to Facebook do appear to consider the possibility of a broad and public audience and take into consideration the range of people who might access their profiles. The perception of online audience appears to shrink, as users continue to explore the Facebook interface, enlarge their social networks, and interact with their friends through these sites.

It is also reported a variety of problems due to lack of usability of Facebook privacy settings. An accidental disclosure that is very difficult for users to detect happens when user's expectations of the outcome of their privacy settings did not match what actually happened. They rarely revisit their privacy pages to ensure settings appropriately cover the growing profile as they continue to expand their profiles by downloading new applications, joining new networks, or disclosing new information.

For sensitive and risky information a solution to over-disclosures is to enforce, or at least default to, more restrictive settings. This may help new users by providing immediate protection, and it may also protect even experienced users while by allowing them to customize their settings to share information when desired. Sensitive information can appear in many profile areas, so new defaults may do not match the desires of users. Privacy controls also need to be more visible, making them accessible while users are modifying their profile instead of located on separate pages. If the user ignores these privacy pages, they will never see their options for modifying the privacy settings.

There is a need to promote correct understanding of the audience of information we are sharing. For improving user's awareness of their profile accessibility initially, certain mechanisms need to be introduced. These mechanisms need to be attached to the regular activities of the users, so privacy does not remain a separate and rare consideration as the user's audience perceptions change.

III. RELATED WORK

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. 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. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. If one of the following two cases is verified true, A3P-core will invoke A3Psocial. The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc). In above cases, it would be beneficial to report to the user the latest privacy practice of social communities that have similar background as the user. The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P-social is invoked, it automatically 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 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 repository of the system for the policy prediction of future uploads.

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 have presented an expressive language for images uploaded in social sites. This work is complementary to ours as we do not deal with policy expressiveness, but rely on common forms policy specification for our predictive algorithm.

Users can express their privacy preferences about their content disclosure preferences with their socially connected users via privacy policies. A tag based access control of data is developed by Peter F. Klemperer. It is a system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends. A suitable preference can be selected by participants and access the information. Based on the user needs photo tags can be categorized as organizational or communicative. There are several important limitations .First, our results are limited by the participants recruited and the photos provided by them. Machine generated access-control rules are the second limitation. Algorithm used here has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. Hence, some rules appeared strange to the participants who makes them to tag explicitly like ―private and public.

Your Privacy Protector is a recommender system proposed by Kambiz Ghazinour that understands the social internet behavior of their privacy settings and recommending reasonable privacy options. The parameters used are user's personal profile, User's interests and User's privacy settings on photo albums .With the help of these parameters the system constructs the personal profile of the user. For a given profile of users it will automatically learn and assign the privacy options. It detects the possible privacy risks and allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors frequently.

Necessary privacy settings are adopted based on these risks.

Privacy Suites is proposed by Jonathan Anderson which allows users to easily choose ―suites" of privacy settings. Using privacy programming a privacy suite can be created by an expert. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. To the members of the social sites the privacy suite is distributed through existing distribution channels. Transparency is the main goal, which is essential for convincing influential users that it is safe to use. The disadvantage of a rich programming language is less understandability for end users. To verify a Privacy Suite sufficiently high-level language and good coding practice, motivated users are able.

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

Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape, texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures.

CONCLUSION

Various privacy policy techniques for user uploaded data and images in content sharing sites are described in this paper. Image content and user behavior determines the privacy policy generation. Present systems have certain advantages as well as disadvantages. The A3P system outperforms other methods but it has a demerit, that is when meta data information about uploaded images are unavailable it is difficult to create privacy policy. Future works lead to automatically annotating images. Automatic image annotation is a challenging problem in multimedia content analysis and computer vision. To annotate images a hierarchical framework is used. An image-filtering algorithm to remove most of the irrelevant images for an unlabeled image is presented first. For the unlabeled image, an image cluster is allocated using a discriminative model as the primary relevant image set in the algorithm. In the second stage, a hybrid annotation model is proposed to annotate images. A baseline method is presented to transfer labels from relevant images to unlabeled image according to global visual features. Regional visual features are extracted to build a probabilistic model for image annotation. Finally, the two annotation results are fused together by a simple weighted algorithm. Experiments have proved this method will provide better results.

REFERENCES

[1] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , I Know What You Did Last Summer !:Privacy-Aware Image Classification and Search‖, Proceedings of the 35th International ACM SIGIR conference on Research and development in information retrieval, 2012.

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

[3] Alessandra Mazzia Kristen LeFevre and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings, Tech. rep., University of Michigan, 2011.

[4] J. Bonneau, J. Anderson, and L. Church, ―Privacy suites: Shared privacy for social networks, in Proc. Symp. Usable Privacy Security,2009

[5] Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek, ―Tag, You Can See It! Using Tags for Access Control in Photo Sharing, Conference on Human factors in Computing Systems, May 2012.

[6] Kambiz Ghazinour, Stan Matwin and Marina Sokolova, Social Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.

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

[8] 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.

[9] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, Capturing social networking privacy preferences, in Proc. Symp. Usable Privacy Security, 2009.

[10] Yuan-yuan ca., Zhi-chun mu, Yan-fei ren ,and Guo-qing xu A Hybrid Hierarchical Framework For Automatic Image Annotation in Proc of the 2014 International Conference on Machine Learning and Cybernetics, Lanzhou, 13-16 July, 2014

[11] A. 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.

[12] R. Agrawal and R. Srikant,"Fast algorithms for mining association rules in large databases," in Proc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.

[13] 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.

[14] M. Ames and M. Naaman, "Why we tag: Motivations for annotation in mobile and online media," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.

