ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

A Survey on the Privacy Settings of User Data and Images on Content Sharing Sites

Sangeetha J

Assistant Professor, Albertian Institute of Management, Cochin, Kerala, India

ABSTRACT: 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 term "social media" refers to the wide range of Internet-based and mobile services that allow users to participate in online exchanges, contribute user-created content, or join online communities. Online social networks are websites that allow users to build 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 contacts and find people with similar interests and ideas.

The relation between privacy and a person's social network is multi-faceted. There is a need to develop more security mechanisms for different communication technologies, particularly online social networks. Privacy is essential to the design of security mechanisms. Most social networks providers have offered privacy settings to allow or deny others access to personal information details. In certain occasions we want information about ourselves to be known only by a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better. Social network theorists have discussed the relevance of relations of different depth and strength in a person's social network and the importance of so-called weak ties in the flow of information across different nodes in a network.

A definition for internet privacy would be the ability to control (1) what information one reveals about oneself, and (2) who can access that information. Essentially, when the data is collected or analyzed without the knowledge or consent of its owner, privacy is violated. When it comes to the usage of the data, the owner should be informed about the purposes and intentions for which the data is being or will be used.

Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings [9], [10]. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone [11], [12].

Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings [2], [4], [13]. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images [14], [5] due to the amount of information implicitly 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 alone can enter the privacy preferences 2.Usage of recommendation systems which assist users for setting the privacy preferences.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

The privacy policy of user uploaded data can be provided based on the user 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. The privacy policy of user uploaded image can be provided based on the user uploaded image's content and metadata. A hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images that do not have metadata will be grouped only by content. Such a hierarchical classification gives a higher priority to image content and minimizes the influence of missing tags.

II. LITERATURE SURVEY

Jonathan Anderson proposed a paradigm called **Privacy Suites [2]** 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.

Fabeah Adu-Oppong developed privacy settings based on the concept of **social circles [3]**. 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 [15].

Kambiz Ghazinour designed a recommender system known as **YourPrivacyProtector [4]** that understands 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 assign the privacy options. It allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. Based on the risks it adopts the necessary privacy settings.

Alessandra Mazzia introduced **PViz Comprehension Tool [5]**, 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 Facebook's Audience View and Custom Settings page.

Peter F. Klemperer developed **a tag based access control of data [6]** shared in the social media sites. 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.

Ching-man Au Yeung propose a access control system based on a **decentralised authentication protocol [7]**, descriptive tags and linked data of social networks in the Semantic Web. It allows users to create expressive policies

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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.

Sergej Zerr propose a technique **Privacy-Aware Image Classification and Search [8]** to automatically detect private images, and to enable privacy-oriented image search. It combines textual meta data images with variety of visual features to provide security policies. 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). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game.

Anna Cinzia Squicciarini developed an **Adaptive Privacy Policy Prediction (A3P) [9]** system, a free privacy settings system by automatically generating personalized policies. The A3P system 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 is inaccurate privacy policy generation in case of the absence of meta data information about the images. Also manual creation of meta data log data information leads to inaccurate classification and also violation privacy.

Paper	Author	Privacy Methods Used	Merits	Demerits
Privacy suites: Shared privacy for social networks	J. Bonneau, J. Anderson, and L. Church	Privacy suites	Transparency	Less understandability for users
Social circles: Tackling privacy in social networks.	A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang	Social Circles Finder	Transparency	Applicable to a limited set of users
The PViz Comprehension Tool for Social Network Privacy Settings	Alessandra Mazzia Kristen LeFevre and Eytan Adar	PViz Comprehension Tool	Ease of use	Less understandability for users
Yourprivacyprotector: A Recommender System For Privacy Settings in Social Networks	Kambiz Ghazinour, Stan Matwinand, Marina Sokolova	Your Privacy Protector	Transparency	Difficulty to understand
Tag, You Can See It! Using Tags for Access Control in Photo Sharing	Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek,	Tag based access control of data	Transparency	Applicable to a limited set of users
Decentralization: The future of online social networking	Ching-man Au Yeung	Tags and linked data	Applicable to multiple content sharing sites	Applicable to a limited set of users
I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search	Sergej Zerr, Stefan Siersdorfer	Privacy-Aware Image Classification and Search	Directly search for private data	Complexity

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites	Anna Cinzia Squicciarini	Adaptive Privacy Policy Prediction	Ease of use	Inaccurate privacy policy generation in case of the absence of meta data information about the images

Table 1. Observation and comparison of Existing System

III CONCLUSION AND FUTURE WORK

This paper describes various privacy policy techniques for user uploaded data and images in various content sharing sites. The privacy policy can be applied based on the user social behavior and the user uploaded image content. Table I presents the overview of various privacy policy techniques among the existing systems. Future research lead towards improving the performance by a novel semantic retrieval of images is done based on Hidden Markov model based annotated images. To annotate the images, features such as Color and texture feature are extracted by using Color Histogram and SIFT Descriptors methods. This method will provide more efficient results.

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 Transactions on Knowledge and Data Engineering, Vol. 27, NO. 1, January 2015.
2. J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.
3. 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.
4. Kambiz Ghazinour, Stan Matwin and Marina Sokolova, "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.
5. Alessandra Mazzia Kristen LeFevre and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings, Tech. rep., University of Michigan, 2011.
6. 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.
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. 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.
9. Anna Cinzia Squicciarini, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions On Knowledge And Data Engineering, vol. 27, no. 1, January 2015.
10. 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.
11. 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.
12. H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.
13. K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput.
14. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.
15. R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
16. 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.
17. Mehmet Erkan Yüksel and Asım Sinan Yüksel, "An Application for Protecting Personal Information on Social Networking Websites", The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2010.

BIOGRAPHY

Sangeetha J is a Research Scholar in the Computer Science Department, PSGR Krishnammal College for women, Coimbatore. She received Master of Computer Application (MCA) degree in 2009 from Annamali University, India. Her research interests are Data mining, computer networks etc.