



Privacy study on images uploaded in social networks

Hemalatha D^{1*}, Almas Begum², Alex David S³

^{1,2}Assistant Professor, ³Associate Professor Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India
*Corresponding author E-mail: hema24294@gmail.com

Abstract

Presently, the growth of Social media is explosive among the users. Increasingly developed social websites like Flickr, Facebook, Google+, LinkedIn etc permits the users to create, share and view the post. Confidentiality is a leading factor required in Social Networks. The social users upload their photos to the social sites that intend to gain public interest for social purposes. The exposure of personal information leads to slipping process like identity stealing, morphing etc, which are against the privacy violations. Relied upon the personal characteristics of users, the privacy settings of each user should be defined. In this paper, a relational study about the privacy settings in Online Social structure is examined. Initiated by the importance of social networks among the social users and their behavior towards Online Social Networks, which is followed by the privacy techniques suggested by other researchers are explored. At last, an overview about the merits and demerits of privacy designs and schemes for the user-uploaded images are presented. The study results a new privacy system that controls the confidential information from being accessed from different devices, including mobile devices and computers.

Keywords: Online Social Structure, Social Media Users, Privacy, Images, And Sensitive Information

1. Introduction

With the advancements in the Online Social Networking, the growth of social media users is inclined. It assists the social users to make new contacts, old friends and sharing the common opinions with the group of people across the world. It acts as communication links among the users. As the increased usage of websites, the participation of user's rate is also increased. By this advent, the user's share their images and personal information to their communities. Without having prior knowledge about the privacy settings, the images are uploaded and shared among the group of people. By doing so, a variety of risks are faced by the social users like identity stealing, morphing etc. Despite these risks, many privacy mechanisms of content sharing sites are very weak.

A profile of a user comprised of details like company details, educational details, residential address, common interest etc. In order to be a part of the networks, tagging concept is emerged. An image of a user is tagged [1] with several people to gain interests. This concept becomes riskier in the complicated environment. And also, the users are unaware about the consequences of tagging concept of an image. Instead of imposing restrictions over such incidents or increasing security, sites like FB and Instagram are encouraging people to get into such things.

Online Social Networking is still in developing stage, but it elegantly supports some eminent applications [2]. As this technology grows, we, eventually, expect some advanced functionalities. It is not incredible that social structure will someday become de-facto portals for both personal and commercial online interactions. Users located adjacent in a social network tend to trust each other more than the users located in random pairs, which is shown in

fig.1. Users browse neighbouring areas of their interpersonal organization as they need to discover important content. Witnessing how content direct these networks over a period of time and ends up prominently increasing important in commercial advertising, in political campaigning, and ultimately to society.

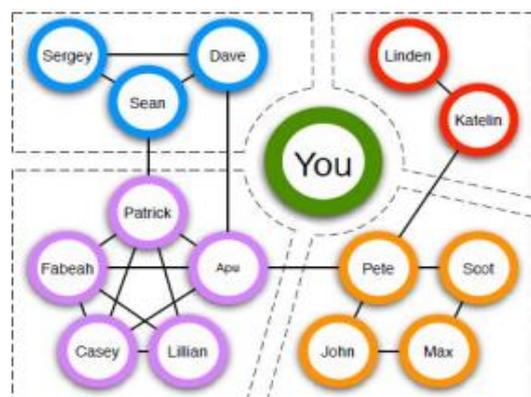


Fig.1. Community formation in Social networks

Further, paper is organized as follows: Section II discusses about the existing schemes suggested by other researchers and Section III discusses with summary of the review findings made in our study.

2. Related Work

In this section, we present a clear idea about the significance of the Online Social Networks, User's behavior in Online Social Network (OSN) and techniques involved.

2.1 SIGNIFICANCE OF OSN

In depths of revolution in social media, it has become vital communication medium. The primary benefit of the social media is the sharing and gaining of knowledge from wide range of people. This kind of growth develops the communication skills towards the online learners. Social media has touched our lives, both on an interpersonal and a community level. These networks grow based on personal interactions over a time and connects users with the technological infrastructure, social know- how as well as technical expertise's.

2.2 USER BEHAVIOR IN ONLINE SOCIAL NETWORKS

The perception towards user behavior in Online Social Networks imposes a better interface design for improved content distributed systems. It is crucial to study about the behavior of users when they are associated to the social websites. Email is considered as important factor for associating with the networks [3]. In current scenario, the social links are interlinked with each other. A single account of user is associated with different social websites. It assists the service providers to identify the attitudes of users. In order to improve the user's experience, the behavior study is an important thing. In section 2.2, we explore the four orientations of defining the user behavior in social networks. The four orientations are as follows:

- Finding the associations between users in OSN using Social Graph
- Monitoring the events for predicting the network traffic
- Development towards mobile platforms and applications
- Security and privacy analysis-based user's behavior

a) Finding the associations between social users:

Social Graph is a mathematical model used for assessing the connections among the social users. It assists us to provide details about the characterization of user's behaviours. The table 1 depicts the knowledge of five eminent social networks.

Table 1. Knowledge about five eminent social networks [9]

SOCIAL SITES	NO. OF USERS In billion
Facebook	1.01
Linkedin	200
Google +	450
Foursquare	30
Twitter	500

Social graph is modelled into two ways, namely, undirected graph model and directed graph model. The four fundamental graphs are listed in Table 2. Relied upon these sorts of graph, the associations among the OSN users are studied. In addition to this, it imposes to research about the efficacy of social graphs. To resolve this issue, the authors in [4], proposed crawling techniques. The friendship graph and interaction graph belong to the class of undirected graph and directed graph model includes latent graph and following graph. Friendship graph is defined that every user is considered as nodes and edge is represented as the connections between users. Therefore, friendship in OSNs can hardly be viewed the same as friendship in the real world. Interaction graph is defined to find the communication between the users in real- world entities. Then, the

conventional measurement approaches are used for understanding the behaviors from browsing. Latent graph is built from the friendship graph and interaction graph. The overall system architecture is given in fig.2.

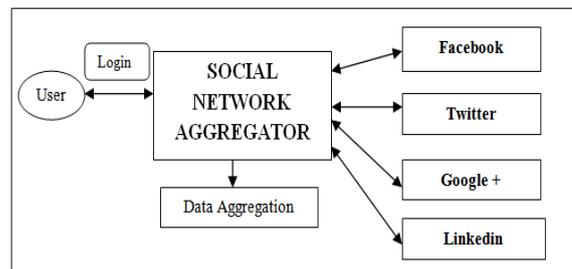


Fig.2. Profiling data through social network aggregator [11]

Table 2. List of different social graphs [12]

SORTS OF GRAPH	EDGE
Friendship Graph	Depicts the associations or connections between users
Interaction Graph	Depicts the posting behaviors
Latent graph	Depicts the browsing profile
Following graph	Depicts to obtain the messages

b) Network Monitoring analysis

A variant kind of social graphs intimates the associations between the users. In some cases, the user's activities can't be predicted due to restricted information about them. Internet service Provider has better understanding about traffic pattern between end user and social network sites and ability to provide optimized solution according to the OSN users. Instead of using crawling techniques, the network events also play a vital role to predict the user's behaviour. As in fig.2, Clickstream data is used for analysing the behaviour from Social Network Aggregator (SNA). Benevenuto et al studied about the user behaviour from Clickstream data analysis. The author in [5] collected user data for a week of time that intended to study about the behavioural aspects of social users.

Atlas, they concluded that the user's browsing data contain: i) Frequency of data access in OSN ii) Aggregate time spent on OSN iii) Session monitoring in OSNs. From their study, they encountered 40 types of user's activities with their traffic bytes [5]. And they also discussed about the user's transition using markov chain model. The study on behaviour of user in OSN is shared by Clickstream data. Due to restriction in usage and performance of data, it is incomplete. The features such as collection duration, behaviour of inactive user, monitoring location also limits the clickstream data.

c) Mobile Application Developments

Mobile platforms are also depicts the behavior of user. A variant number of web applications are emerged, so it is necessary to study about the mobile social networks. Some social websites also permits to access the data from mobile networks. In order to design mobile systems, the behavioral study of user is also important. By the advent of Bluetooth [6], the nearby users are recognized and the data is shared among them. This is referred as the social serendipity. For example, internal collaboration in companies can be sophisticated by serendipity for bringing the people working in the similar project together. The serendipity is fundamentally emphasized with privacy issues and tools related to it must be designed with care.

Table 6: Relational study of merits and demerits of privacy analysis

Techniques for privacy	Merits	Demerits
Design oriented privacy suites	Design policies are transparent in nature.	Difficult to understand by normal users
Study on social circles	Flexible for finding association among the users.	Unable to process for higher number of users.
Compression schemes for images	Simple to use	Overhead in computational process
Privacy protector tools	Transparent process	Highly difficult to understand
Tagging concepts	Transparent process	Inefficient handling of large set of users.
Linked data to the tags and keywords	Link with multiple sites	Limited set of connecting the linked data
Image classification and search for privacy schemes	Performs direct search for protected data	High complexity

3. Conclusion

Nowadays, a vast amount of private data is being shared in the social networking sites. The private data includes sensitive information and images, in which images are being mostly shared by most of the social users. In order to eliminate the malicious events, a well-reputed privacy schemes are required. But, in most of the cases, applying privacy schemes on the data is a cumbersome task. In this paper, relational study of privacy settings in Online Social Networks is examined. In specific to, we studied about the privacy settings for the user-uploaded images.

From this study, we summarized that the privacy oriented importance given to the user-uploaded images are not yet flourished. It is wisely recommended that a privacy design for user-uploaded images need to be developed. The privacy systems of Online Social Networks should accommodate their users with different levels of privacy settings for their images irrespective of location and time.

References

- [1] White, T.; Chu, W.; Salehi-Abari, A.; "Media Monitoring Using Social Networks," Social Computing (Social Com), 2010 IEEE conferences on Social networking sites, 2010, pp.661-668.
- [2] Rodrigues, E.M.; Milic-Frayling, N.; Fortuna, B.; "Social Tagging Behavior in Community-Driven Question Answering," Web Intelligence and Intelligent Agent Technology, 2008, pp.112-119.
- [3] Nielsen Online Report, "Social networks & blogs now 4th most popular online activity", 2009.
- [4] C. Wilson et al., "User Interactions in Social Networks and Their Implications," Proc. EuroSys, 2009.
- [5] F. Benevenuto et al., "Characterizing User Behavior in Online Social Networks," Proc. IMC, 2009.
- [6] F. Schneider et al., "Understanding Online Social Network Usage from a Network Perspective," Proc. IMC, 2009.
- [7] Campisi, P.; Maiorana, E.; Neri, A., "Privacy protection in social media networks a dream that can come true?," 16th International Conference on Digital Signal Processing, vol., no., pp.1,5, 2009
- [8] Rosenblum, D., "What Anyone Can Know: The Privacy Risks of Social Networking Sites," Security & Privacy, IEEE,
- [9] Novak, E. & Li, Q., "A Survey of Security and Privacy in Online Social Networks", College of William and Mary Computer Science Technical Report, WM-CS-2012-2
- [10] J. Bonneau, J. Anderson, and L. Church. Privacy suites: shared privacy for social networks. In Symposium on Usable Privacy and Security, 2009.
- [11] A. K. Fabeah Adu-Oppong, Casey Gardiner and P. Tsang, "Social circles: Tackling privacy in social networks", In Symposium On Usable Privacy and Security, 2008.
- [12] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive policy prediction for shared images over popular content

sharing sites," inProc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp.261-270.

- [13] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," inProc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111-119.
- [14] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," inProc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9-14.
- [15] 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.
- [16] M. Wittie et al., "Exploiting Locality of Interest in Online Social Networks," Proc. CoNext, 2010.