

# A Study on Privacy Conflicts in Social Media

J.Jananipreetha<sup>#1</sup>, Dr. P. Ponmuthuramalingam<sup>#2</sup>

<sup>#1</sup>M.Phil Research Scholar, PG & Research Department of Computer Science,  
Government Arts College (Autonomous),  
Coimbatore, INDIA

<sup>#2</sup>Associate Professor in Computer Science and Controller of Examinations,  
Government Arts College (Autonomous),  
Coimbatore, INDIA

<sup>1</sup>jananipreetha1991@gmail.com

**Abstract-** Online Social Networks (OSNs) plays an important role in Social media. It has tremendous growth in recent years. Social networks help users to socialize and share content with other users. These OSNs produce a number of security issues and privacy. Online social networks (OSNs) have greatly transformed the online performance and activities of users. Unfortunately such services have also proposed a number of privacy issues. As the use of these services covers across multiple aspects of daily life, users may face many consequences when their personal and professional life can disturb each other via OSNs. . The lack of multi-party privacy management in Social Media makes users unable to control to whom these items are really shared or not. In this survey, focus is on review about privacy conflicts in social media.

**Keywords--**Online Social Networks, Privacy Conflicts, data sharing

## I. INTRODUCTION

Social networks are online applications that permit the users to connect by way of various link types. Privacy has become one of the most research issues. Unfortunately, privacy has not been fully focused yet. People are not cautious in releasing their personal information. An important privacy threat is developed by an increasing volume of media content posted by users in their profile. People posted their pictures to other users. Such pictures are made accessible for other Social Network who can view and specify the users who appear in the pictures [2]. In current SNs, when uploading a picture, user is not essential to ask for permissions of other users appearing in the photo, even if they are explicitly recognized through tags. Although most social networking and photo sharing websites provide methods and default structures for data sharing control [6].

## II. LITERATURE REVIEW

Besmer et al[2] proposed Photo privacy when sharing and tagging images. Photo tagging is a popular aspect of many social network sites that allows users to uploaded images

openly linking the photo to each person's profile. This examines privacy concerns and mechanisms surrounding these tagged images. Using a focus group, it studied the needs of users, resulting in a set of design considerations for tagged photo privacy and then designed a privacy enhancing mechanism based on Findings, and authenticated it using a mixed methods of approach. Results identify the social tensions that tagging produces, and the needs of privacy tools to address the social implications of photo privacy management.

Wisniewski et al [3] paper emphases specifically on how users try to overcome their privacy needs. Therefore, improved interface design to better support interpersonal boundary regulation could serve to improve, instead of prevent, higher levels of social interaction. Future research will continue along this path - to examine interpersonal boundary regulation within online social networks as a means to align interactional privacy needs with social networking goals.

Hu et al [5] presents a efficient solution of shared data in OSNs. Some typical data sharing patterns with multiparty authorization in OSNs are also recognized. Based on the sharing patterns, an MPAC (Multiparty Access Control) model is devised to capture the core features of multiparty authorization. An MPAC mechanism can greatly improve the flexibility for controlling data sharing in OSNs, it may potentially reduce the certainty of

system authorization and privacy conflicts need to be resolved easily. It explore a comprehensive solution to cope with collusion attacks for delivering a robust MPAC service in OSNs.

J. M. Such et al[4] introduces the problem of preserving privacy in computer applications and its relative to autonomous agents and Multi-agent Systems. It also

reviews privacy-related studies in the field of Multi-agent Systems and characterizes open challenges to be addressed by future research and introduced the issue of privacy preservation and its relation to Multi-agent Systems. Thus, approaches based on concepts that can further improve privacy in other existing technologies.

Wishart et al [6] present a solution to this problem that employs a shared method for specifying privacy policies and presented a novel approach to collaborative policy authoring demonstrated within the context of social networking. Collaborative access control framework that enables multiple controllers of the shared item to collaboratively state their privacy settings and to resolve the conflicts among co-controllers with different requirements and desires. This methodology presents a policy specification plan for collaborative access control and authorization administration. It is important to have mechanism for collaborative management of privacy settings for shared data.

Squicciarini et al [7] present a policy specification scheme for collaborative access control and authorization administration. Based on these considerations, algorithms are devised to achieve a collaborative access control policy over who can access or disseminate the shared item or not access the shared item. It also introduces analyze scenarios, where more than one user should be involved in the process of making a collective access control policy.

Hoang-Giang Do et al [8] introduce crypto-based framework for structure online social networking services to overcome privacy issues. It permits users to numerically sign and encode their posted content at the client side before moving it to the server so that it guarantees privacy. It aims to help users to protect privacy and integrity of the data. It state conventions about the threat mode, and use them to affect the goals of system design. The proposed model must assurance that a user is able to detect misbehavior from the server.

**TABLE 1**

**COMPARISON OF PRIVACY POLICY AND ITS CONFLICTS**

<b>S.NO.</b>	<b>TITLE</b>	<b>MECHANISM/POLICY</b>	<b>FEATURE</b>
1	Collaborative privacy policy in a social networking context	PRiMMA Viewer Prototype (privacy aware Content sharing application)	Privacy in uploading content
2	Fighting for my space: Coping mechanism for SNS boundary regulation	Coping mechanism	Boundary Regulation for managing interpersonal boundaries
3	Collaborative privacy management in social networks	Private box approach	controlled sharing of pictures
4	Privacy preserving social network for an untrusted server	Crypto based framework	Protect the privacy and integrity of their data
5	Moving Beyond Untagging: Photo Privacy in a Tagged World	Privacy enhancing mechanism	Photo privacy management
6	Multiparty Access Control for Online Social Networks: Model and Mechanisms	Access control	Secure image sharing and tagging

### III. CONCLUSION

Privacy plays an important role in social media. The survey presents various studies related to privacy conflicts in social network. An MPAC model [Hu et al] provide best mechanism and solution to the privacy issues in the aspects of access control mechanism. The mechanism has been used to provide secured sharing and tagging images with access control. It provides a basic guide to help experts understand privacy rights related to the use of social networking sites.

### IV. REFERENCES

- [1] Internet.org, “A focus on efficiency,” <http://internet.org/efficiencypaper>, Retr. 09/2014.
- [2] A. Besmer and H. Richter Lipford, “Moving beyond untagging: photo privacy in a tagged world,” in ACM CHI, 2010, pp. 1563–1572.
- [3] P. Wisniewski, H. Lipford, and D. Wilson, “Fighting for my space: Coping mechanisms for sns boundary regulation,” in Proc. CHI. ACM, 2012, pp. 609–618.
- [4] J. M. Such, A. Espinosa, and A. García-Fornes, “A survey of privacy in multi-agent systems,” The Knowledge Engineering Review, vol. 29, no. 03, pp. 314–344, 2014.
- [5] H. Hu, G. Ahn, and J. Jorgensen, “Multiparty access control for online social networks: model and mechanisms,” IEEE TKDE, 2013.
- [6] R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, “Collaborative privacy policy authoring in a social networking context,” in POLICY. IEEE, 2010, pp. 1–8.
- [7] A. Squicciarini, M. Shehab, and F. Paci, “Collective privacy management in social networks,” in WWW. ACM, 2009, pp. 521–530.
- [8] Hoang-Giang Do, Wee-Keong Ng and Zhedong Ma, “Privacy-Preserving Social Network for an Untrusted Server”, IEEE Third International Conference on Cloud and Green Computing 2013.