IJARES/October 2014/Volume-2/Issue-10/1681-1685 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

UNDERTAKING OF PRIVACY ISSUES CONCERNING SOCIAL NETWORK

Shaik Mahaboob Johny[1], Shaik Habeeba[2]

[1]**M.Tech Student, Dept of CSE, Nimra Institute of Engineering & Technology, Ongole, A.P, India**

[2]**Assistant Professor, Dept of CSE, Nimra Institute of Engineering & Technology, Ongole, A.P, India**

ABSTRACT:

Social network provider has access towards user content and authority to decide who might have access to information. Social privacy concerns towards issues that users elevate and practice when technically mediated communications disturb social limits. Traditional limits that cause social communications might be disrupted while novel ones might come into being. Privacy settings permit users to articulate their preferences regarding revelation and cover up of their information. Privacy enhancing technologies frequently used to explain a broad range of privacy explanations; refer to technologies specially intended to defend citizens' online privacy in the direction of overbearing conditions and collaborating service providers.

Keywords: Social network, Privacy enhancing, Social privacy, User.

1. INTRODUCTION:

The social tagging relating to people of social network enhances visual legibility of social network users which is used in support of surveillance purpose. Various research studies illustrate that online social network users struggle with a variety of issues such as dented reputations, interpersonal variances, redundant contacts, context collision, blackmailing and so on [1]. Each user articulate other users list through whom a relationship is shared and it comprises an extensive range of tools for people to put together an understanding of neighbourhood in an unofficial and intended way. Many networks are represented in

communities and are developed within the characteristic organizational structures that are supposed to support the normal flow of work. Networks may be very dynamic or stable and the users are continually combining or leaving the networks based on changing interests. Privacy settings are intended to defend a user from further members of the social network [2]. Three types of privacy problems were differentiated that researchers in computer science undertake and the initial approach addresses the problem of surveillance that happens when the personal data and social connections of online social network users are leveraged by means of providers of governments. The second approach tackles those problems that come into view through the essential renegotiation of limits as social interactions get reconciled by online social network services, briefly known as social privacy [3]. The third approach tackles efforts related to users losing control and misunderstanding over the assortment and processing of their information in online social networks known as institutional privacy.

2. METHODOLOGY:

Providers of social networks have access towards each and every user made content and power to decide who might have access to information and leads to social privacy problems. Research of computer science on institutional privacy revise ways of recovering organizational data management practice in support of compliance, for instance by developing mechanism for control of information flow as well as accountability in back end. The individuals who are in interaction with others can add information to the data space and make their contribution in different interactive actions [4]. An online social networking can be represented by an association network, a set of user groups and an assortment of user information shown in fig1. Researchers do not on the other hand learn how issues of social privacy might reconfigure organizational data management precise to social networks. Most significantly, rarely do researchers across three communities' team up to concentrate on these divergences. Researchers working from various stand point be different not only in what they abstract, however also in their elementary assumptions concerning what privacy problem is. Given the efficiency and

accomplish of the Internet, and the track evidence of surveillant grouping some privacy researchers believe that it may possibly not be enough to rely exclusively on the legal method to look after their citizens. They thus recommend solutions that contradict such surveillant assemblages all the way through an additional type of code such as software itself and this is one of secure points for technological privacy solutions which are known as privacy enhancing technologies [5]. Social privacy relates to the issues that users elevate and to the harms that they practice when technically mediated communications disturb social limits. Conventional limits that motivate social communications might be disrupted while novel ones might come into being. These might be boundaries among private and public, the intimate and remote, directness in addition to closeness. Popular accounts of privacy contravention in news media have finished social privacy problem and these privacy problems have been deliberate by a diversity of research communities in and clear of computer science. Researchers have exposed that way precision, involvement is entrenched into social network design play a significant role in way information flows in networked system. These novel flows of information might weaken the spatial as well as temporal assumptions that material world communication depends on.

3. ACCESSING INFORMATION ON SOCIAL NETWORKS:

The problems of surveillance, social privacy, and institutional privacy finish up being treated as if they were autonomous phenomenon. In the same way, the problems of surveillance are not autonomous of social privacy. Social practices in online social networks may possibly have consequences for the efficiency of measures of intrusive surveillance. Consequently, a several privacy problems users practice with might not be due to their individual actions, but as a substitute result from tactical design changes put into practice by social network provider. Privacy enhancing technologies frequently used to explain a broad range of privacy explanations; refer to technologies specially intended to defend citizens' online privacy in the direction of overbearing conditions and collaborating service providers. The prominence of Privacy enhancing technologies is consequently on preventing revelation of user information, with supposition that controlling how

information is utilized subsequent to disclosure is not possible. The complexity of control after revelation is finest illustrated by social network privacy settings. Privacy settings permit users to articulate their preferences regarding revelation and cover up of their information. These settings however do not enclose options in support of hiding information from social network provider itself, who by design has access towards information of all users. While cryptography preserve privacy of the user produced content uploaded towards social network, it does not cover up user connections as well as behaviour [6]. The method of transparency and sharing is entrenched into design of online social networks plays a significant role in the means information flows in networked systems. These new flows of information may possibly challenge the spatial and temporal statements that physical world communication relies on. Privacy enhancing technologies grew out of cryptography as well as computer security exploration, and consequently designed security engineering principles, for instance threat modelling as well as security analysis. Classical security knowledge was developed in support of national security purpose, and later on, for protecting commercial information as well as transactions. They were supposed to look after state as well as corporate secrets, and to defend organizational process from disruptions. The privacy struggles addressed by Privacy enhancing technologies are in numerous ways a reformulation of previous security threats, for instance confidentiality breaches or else denial of service attacks. The purpose of Privacy enhancing technologies in circumstance of social networks is to facilitate individuals to connect with others, distribute, as well as bring out information online, at no cost from surveillance as well as interference.

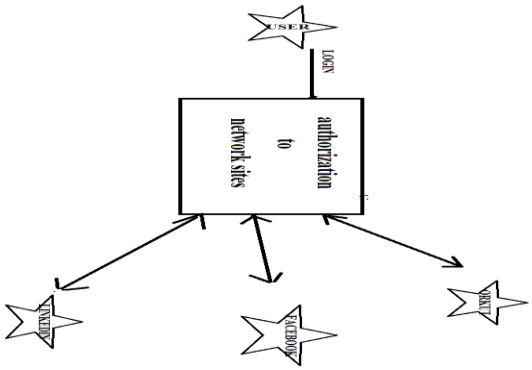

Fig 1: An overview of social networking.

4. CONCLUSION:

Various research studies illustrate that online social network users struggle with a variety of issues such as dented reputations, interpersonal variances, redundant contacts, context collision, blackmailing and so on.

The individuals who are in interaction with others can add information to the data space and make their contribution in different interactive actions. Many networks are represented in communities and are developed within the characteristic organizational structures that are supposed to support the normal flow of work. Privacy settings are intended to defend a user from further members of the social network. The problems of surveillance, social privacy, and institutional privacy finish up being treated as if they were autonomous phenomenon. In the same way, the problems of surveillance are not autonomous of social privacy. Social practices in online social networks may possibly have consequences for the efficiency of measures of intrusive surveillance. Privacy enhancing technologies frequently used to explain a broad range of privacy explanations; refer to technologies specially intended to defend citizens' online privacy in the direction of overbearing conditions and collaborating service providers.

REFERENCES

[1] E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams. Hummingbird:

Privacy at the time of twitter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.

[2] A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, 47(12):94–101, 2009.

[3] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The secondgeneration onion router. In USENIX Security Symposium, pages 303– 320, 2004.

[4] FTC. Ftc charges deceptive privacy practices in google's rollout of its buzz social network. Online, 03 2011.

[5] Glenn Greenwald. Hillary clinton and internet freedom. Salon (Online), 9. December 2011.

[6] James Grimmelmann. Saving facebook. Iowa Law Review, 94:1137– 1206, 2009.