ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Privacy Protection & Surveillance over Online and Mobile Social Networking Sites.

Malipeddi Kishore
M.Tech Student,
Department Of Computer Science Engineering,
Aditya Institute Of Technology And Management,
Tekkali.

MVB Chandra Sekhar
Associate Professor,
Department Of Computer Science Engineering,
Aditya Institute Of Technology And Management,
Tekkali.

Abstract:

Mobile social networking is social networking where individuals with similar interests converse and connect with one another through their mobile phone and/or tablet. Much like web-based social networking, mobile social networking occurs in virtual communities. A current trend for social networking websites, such as Facebook, is to create mobile apps to give their users instant and real-time access from their device. Safety issues (including security, privacy, Surveillance and trust) in Online and mobile social networks are concerned about the condition of being protected against different types of failure, damage, error, accidents, harm or any other non-desirable event, while mobile carriers contact each other in mobile environments. However, lack of a protective infrastructure in these networks has turned them in to convenient targets for various perils.

This is the main impulse why OSNs and MSNs carry disparate and intricate safety concerns and embrace divergent safety challenging problems. Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. Surveillance is also considered and discussed in this paper. The rationale behind this work paper is to investigate the threats to privacy that come up while users not have a good judgment of privacy consciousness and apprehension when using social networking sites. This particular approach, though, clashes with users' increasing privacy concerns regarding revealing their individual profiles to absolute unfamiliar persons.

Keywords: Online Social Networks(OSNs), Mobile Social Networks(MSNs), Privacy, Surveillance, Individual Profiles, Privacy Protection, Information encryption.

Introduction:

Privacy is one of the friction points that emerge when communications get mediated in Online Social Networks (OSNs). Different communities of computer science researchers have framed the 'OSN privacy problem' as one of surveillance, institutional or social privacy. In tackling these problems they have also treated them as if they were independent. We argue that the different privacy problems are entangled and that research on privacy in OSNs would benefit from a more holistic approach. In this article, we first provide an introduction to the surveillance and social privacy perspectives emphasizing the narratives that inform them, as well as their assumptions, goals and methods. We then juxtapose the differences between these two approaches in order to understand their complementarity, and to identify potential integration challenges as well as research questions that so far have been left unanswered.

A social networking service is a platform to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social networks are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as mobile connectivity, photo/video/sharing and blogging.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

More and more, the line between mobile and web is being blurred as mobile apps use existing social networks to create native communities and promote discovery, and web-based social networks take advantage of mobile features and accessibility. As mobile web evolved from proprietary mobile technologies and networks, to full mobile access to the Internet, the distinction changed to the following types:

1) Web based social networks being extended for mobile access through mobile browsers and smartphone apps, and

2) Native mobile social networks with dedicated focus on mobile use like mobile communication,location-based services, and augmented reality, requiring mobile devices and technology. However, mobile and web-based social networking systems often work symbiotically to spread content, increase accessibility and connect users from wherever they are.

Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information and the threat of sexual predators. Users of these services also need to be aware of data theft or viruses. However, large services, such as MySpace and Netlog, often work with law enforcement to try to prevent such incidents.In addition, there is a perceived privacy threat in relation to placing too much personal information in the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken.

Furthermore, there is an issue over the control of data—information that was altered or removed by the user may in fact be retained and passed to third parties. This danger was highlighted when the controversial social networking site Quechup harvested e-mail addresses from users' e-mail accounts for use in a spamming operation.

Privacy on social networking sites can be undermined by many factors. For example, users may disclose personal information, sites may not take adequate steps to protect user privacy, and third parties frequently use information posted on social networks for a variety of purposes.

"For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information".

Privacy Threats:

- Privacy implications associated with online social networking depend on the level of identifiability of the information provided, it's possible recipients, and its possible uses.

- Face Identification.

- Demographic data.

- It is relatively easy for anyone to gain access to it. By joining the network, hackingthe site, or impersonating a user by stealing his password.

- Stalking to identity theft.

- Personal data is generously provided and limiting privacy preferences are sparinglyused.

- Due to the variety and richness of personal information disclosed in Facebook profiles, their visibility, their public linkages to the members' real identities, and thescope of the network, users may put themselves at risk.

- Building Digital Dossier.

Privacy concerns have been found to differ between users according to gender and personality. Women are less likely to publish information that reveals methods of contacting them. Personality measures openness, extraversion, and conscientiousness were found to positively affect the willingness to disclose data, while neuroticism decreases the willingness to disclose personal information.

Many social networks provide an online environment for people to communicate and exchange personal information for dating purposes. Intentions can vary from looking for a one time date, short-term relationships, and long-term relationships.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Most of these social networks, just like online dating services, require users to give out certain pieces of information. This usually includes a user's age, gender, location, interests, and perhaps a picture. Releasing very personal information is usually discouraged for safety reasons. This allows other users to search or be searched by some sort of criteria, but at the same time people can maintain a degree of anonymity similar to most online dating services. Online dating sites are similar to social networks in the sense that users create profiles to meet and communicate with others, but their activities on such sites are for the sole purpose of finding a person of interest to date. Social networks do not necessarily have to be for dating; many users simply use it for keeping in touch with friends, and colleagues.

However, an important difference between social networks and online dating services is the fact that online dating sites usually require a fee, where social networks are free. This difference is one of the reasons the online dating industry is seeing a massive decrease in revenue due to many users opting to use social networking services instead. Many popular online dating services such as Match.com, Yahoo Personals, and eHarmony.com are seeing a decrease in users, where social networks like MySpace and Facebook are experiencing an increase in users.

One common form of surveillance is to create maps of social networks based on data from social networking sites such as Facebook, MySpace, Twitter as well as from traffic analysis information from phone call records such as those in the NSA call database, and others. These social network "maps" are then data mined to extract useful information such as personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities.

Some people believe that the use of social networking sites is a form of "participatory surveillance", where users of these sites are essentially performing surveillance on themselves, putting detailed personal information on public websites where it can be viewed by corporations and governments. In 2008, about 20% of employers reported using social networking sites to collect personal data on prospective or current employees.

Existing System:

Privacy protection is an important study topic in Mobile social networking. The social networking platforms are comprehensive of the mobile environment, users need more widespread privacy-preservation for the reason that they are new with the neighbors in surrounding area who may store, and compare their personal information at different time periods and locations.

Once the private data is associated to the location information, the actions of users will be totally revealed to the general public. To overcome the privacy violation in OSNs and MSNs, many privacy enhancing techniques have been adopted into the OSN & MSN applications.

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

Threats in Online & Mobile Social Networks:

1. Digital record aggregation: Profiles on OSNs & MSNs can be downloaded and stored by third parties, creating a digital record of private data.

2. Secondary data collection: Information knowingly revealed in a profile. Various researches propose that such data is being used to significant monetary gain.

3. Face recognition: User-provided digital images are a very popular part of profiles on MSNs. The picture is, in effect, a binary identifier for the user, allowing linking across profiles..

4. Difficulty of complete account deletion: Users aspiring to remove accounts from OSNs & MSNs discover that it is more or less not possible to delete secondary information linked to their profile such as public comments on other profiles.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

5. Difficult to guard from malicious users who are snooping about the personal information of other users.

6. Difficult to safeguard from neighbors in mobile environment who may snoop, store, and compare their personal information.

7. The Internet stores an everlasting record of the conversation which can be tracked.

8. Using non-secure passwords might perhaps be without difficulty guessed by cyber criminals and compromise your OSN & MSN account to spam your contacts.

Proposed System:

We distinguish three types of privacy problems that researchers in computer science tackle. The first approach addresses the "surveillance problem" that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers. The second approach addresses those problems that emerge through the necessary renegotiation of boundaries as social interactions get mediated by OSN services, in short called "social privacy". The third approach addresses problems related to users losing control and oversight over the collection and processing of their information in OSNs, also known as "institutional privacy".

MODULE DESCRIPTION:

Number of Modules After careful analysis the system has been identified to have the following modules:

1.The Social Privacy Module.

2.Surveillance Module.

3.Institutional Privacy Module.

4.Approach To Privacy As Protection Module.

1.The Social Privacy Module:

Social privacy relates to the concerns that users raise and to the harms that they experience when technologically mediated communications disrupt social boundaries.

The users are thus "consumers" of these services. They spend time in these (semi-)public spaces in order to socialize with family and friends, get access to information and discussions, and to expand matters of the heart as well as those of belonging. That these activities are made public to 'friends' or a greater audience is seen as a crucial component of OSNs. In Access Control, solutions that employ methods from user modeling aim to develop "meaningful" privacy settings that are intuitive to use, and that cater to users' information management needs.

2.Surveillance Module:

With respect to surveillance, the design of PETs starts from the premise that potentially adversarial entities operate or monitor OSNs. These have an interest in getting hold of as much user information as possible, including user-generated content (e.g., posts, pictures, private messages) as well as interaction and behavioral data (e.g., list of friends, pages browsed, 'likes'). Once an adversarial entity has acquired user information, it may use it in unforeseen ways – and possibly to the disadvantage of the individuals associated with the data.

3.Institutional Privacy Module:

The way in which personal control and institutional transparency requirements, as defined through legislation, are implemented has an impact on both surveillance and social privacy problems, and vice versa. institutional privacy studies ways of improving organizational data management practices for compliance, e.g., by developing mechanisms for information flow control and accountability in the back end. The challenges identified in this paper with integrating surveillance and social privacy are also likely to occur in relation to institutional privacy, given fundamental differences in assumptions and research methods.

4.Approach To Privacy As Protection Module:

The goal of PETs ("Privacy Enhancing Technologies") in the context of OSNs is to enable individuals to engage with others, share, access and publish information online, free from surveillance and interference. Ideally, only information that a user explicitly shares is available to her intended recipients, while the disclosure of any other information to any other parties is prevented.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Furthermore, PETs aim to enhance the ability of a user to publish and access information on OSNs by providing her with means to circumvent censorship.

Conclusion:

In this paper, I studied the aspect of surveillance and Privacy Protection. It is important to see the inter dependence and correlation of Surveillance and Privacy Protection, rather than work them as if they are two completely different issues.

REFERENCES:

[1]Seda Gurses and Claudia Diaz, Two tales of privacy in online social networks IEEE Security & Privacy 11(3):29-37,May/June 2013.

[2].F. Beato, M.Kohlweiss , and K.Wouters. Scramble! your social network data. In Privacy Enhancing Technologies Symposium, PETS 2011, volume 6794 of LNCS, pages 211–225. Springer, 2011.

[3] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano. Privacy-Enabling Social Networking over Untrusted Networks. In ACM Workshop on Online Social Networks (WOSN), pages 1–6. ACM, 2009.

[4] E. De Cristofaro, C. Soriente, G. Tsudik, and A.Williams. Humming- bird: Privacy at the time of twiter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.

[5] 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.

[6] Deirdre K. Mulligan and Jennifer King. Bridging the gap between privacy and design. Journal of Constitutional Law, 14(4):989 – 1034, 2012.

[7] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In CHI '03, pages 129 – 136, 2003.

[8] Kate Raynes-Goldie. Privacy in the Age of Facebook: Discourse, Architecture, Consequences. PhD thesis, Curtin University, 2012.

[9] Rula Sayaf and Dave Clarke. Access control models for online social Inet works. In Social Network Engineering for Secure Web Data and Services. IGI - Global, (in print) 2012.

[10] Fred Stutzman and Woodrow Hartzog. Boundary regulation in social media. In CSCW, 2012.

[11] Irma Van Der Ploeg. Keys To Privacy. Translations of "the privacy problem" in Information Technologies, pages 15–36. Maastricht: Shaker, 2005.

[12] Deirdre K. Mulligan and Jennifer King. Bridging the gap between privacy and design. Journal of Constitutional Law, 14(4):989 – 1034, 2012.

[13] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. InCHI '03, pages 129 – 136, 2003.