# PRIVACY IN SOCIAL NETWORKING WEBSITES

**Dr. N. Jayalakshmi[1], R.G. Kavitha[2]**

*[1] Professor, Dept. of Computer Applications, Saveetha Engineering College, Chennai, India.*
*[2] Assistant Professor, Dept. of Computer Applications, RNS First Grade College, Bangalore, India.*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract -** Millions of internet users spend their time on Social Networking Sites by Chatting, blogging, commenting, posting photo. Social Networking Sites also allow users to easily share video and photography content online. Online interaction and sharing of personal information in social networking sites has raised new privacy concerns. Social Networking Sites (SNS) become a central repository of personal information. It attracts the attention of business, corporate and marketing people. As most of the SNS users' profiles are publicly visible, it is very easy to obtain a particular user's personal information without his concern As a consequence, SNS users expose themselves to different privacy risks. This paper aims to understand the impact of privacy concerns in the context of SNS.

***Keywords:*** *Privacy, Social Networking Sites, threats to privacy, privacy enhancing technologies*

## 1. Introduction

In recent years, Social Networking Sites have witnessed thriving popularity. SNSs are built on real-world social relationships and they have changed the rules of social interaction and communication. They provide their users with a wide variety of virtual-interaction mechanisms. As SNSs have integrated into society's daily life, the privacy risks accompanying such social interaction and communication have raised concerns in social life, industry, academia, and government. This paper discusses the various privacy issues in SNSs.

## 2. Social Networking Sites

Boyd and Ellison define Online Social Networking websites as

"An OSN is a web-based service that allows individuals to

- construct a public or semi-public profile within the service,
- articulate a list of other users with whom they share a connection,
- view and traverse their list of connections and those made by others within the service" [1].

### 2.1 Psychologists' view

- Be aware it is a space that is watched.
- Facebook is transformed from a public space to a behavioral laboratory.
- Privacy is a big issue for the research world. Facebook especially, and Microsoft, is scared to death about privacy issues. A bunch of researchers have access to everybody's posts and Facebook is built on what's yours is private. They are struggling with the problem the same way as the scientific community [2].

### 2.2 Typical behavior in SNS

- In Social Networking Sites users share their information with their friends, family and colleagues. Nearly all the participants involve in the following four activities.
- Post information or messages about themselves or their activities;
- Read information or messages of their friends;
- Browse pictures that friends or others post;
- Post pictures [3].

## 3. Privacy and Privacy Concerns

The word privacy is derived from a Latin word **"PRIVARE"**, which means to separate. Privacy is a fundamental human right to be let alone. In Alan Westin book "Privacy and Freedom" stated four states of privacy: solitude, anonymity, reserve and intimacy. Privacy center gives six pragmatic dimensions of privacy: the right to be left alone, limited access to self, secrecy, and control over personal information about oneself, personhood and intimacy. Decew developed a three dimensional definition: Informational, accessibility and expressive privacy. Burgoon grouped privacy into four relevant categories- physical privacy, social or interactional privacy, psychological privacy and informational privacy.

- Information privacy refers to "the ability of the individual to personally control information about one's self".
- Burgoon and Westin defined information privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves (will be released) is communicated to others".
- Dinev and Hart defined Internet privacy concerns as "concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent in particular". Smith used two dimensions- both central and tangential- that have been identified indifferent domain (e.g., law) to describe privacy concerns.
- Campbell referred Information privacy concern to an individual's subjective views of fairness within the context of information privacy [4].

## 4. Privacy and demographic characteristics

Demographic characteristics are related to privacy. Demographic characteristics are gender, education, income, age.

- Gender is frequently related to privacy perceptions. Males have been found to be more likely to post risqué pictures and are less concerned than females.
- An email survey reveals that users with less education are found to be less concerned with online privacy.
- Internet users with higher incomes were less concerned with online privacy.
- Older Internet users are more polarized in their attitudes to online privacy than younger users. Internet users of age between 25 and 54 are most concerned about their privacy [5].

## 5. Privacy and non- demographic characteristics

- Non-demographic characteristics that affect online privacy areas are concern about privacy, computer skills, bad experiences, the number of SNS sites used and individual psychological characteristics.
- Privacy concerns reduce information disclosure and it may be a moderating factor between personality traits and information disclosure.
- Internet users with higher online skills have a lower fear of information disclosure. But they have a reduced trust in online institutions to protect their personal information.
- Internet users who experienced personal privacy invasions (unwanted advances, stalking, or harassment; damaging gossip or rumors; and having personal data stolen or abused by others) are more likely to have changed their privacy settings than other internet users.
- Internet users with higher privacy concerns used fewer applications but they disclosed more information in those fewer applications.
- Internet users who use SNS for socializing are more likely to disclose information online [5].

## 6. User Expectations

Users have strong expectations for privacy on SNS. Privacy expectations in SNS are based on the relationships friends, networks and also public visibility.

### 6.1 Friends

Friendship is an important characteristic of SNS. Friends can access personal data. Both the parties should accept to have a friendship. Some SNSs may give permission to access the data from the second or third degrees of connection.

### 6.2 Networks

We can also define regions in SNS that can be considered as a network. Privacy controls can be associated only with the defined regions. E.g., Friendster users can limit their profile visibility to certain continents.

### 6.3 Public Visibility

SNS allow user to define some subset of profile data (e.g. Username) visible for searching and identification. Most of the SNSs allow users to relax or strengthen their definition of public information [6].

## 7. Privacy Breach

There are two reasons for privacy breach in SNS:

- Leakage of personal information due to poor privacy settings.
- Leakage of personal information to third party application [7].

## 8. Threats to Privacy

Every minute of the day:

- 100,000 tweets are sent
- 684,478 pieces of content are shared on Facebook
- 2 million search queries are made on Google
- 48 hours of video are uploaded to YouTube
- 47,000 apps are downloaded from the App Store
- 3,600 photos are shared on Instagram
- 571 websites are created
- $272,000 is spent by consumers online (source: All Twitter)

The increasing sophistication of information technology is posing significant threats to SNS users' privacy. These threats can be classified into four categories: Classic threats, Modern threats, Combination threats, Threats targeting children.

### 8.1 Classic Threats

Classic threats are privacy and security threats that not only threaten SNS users but also Internet users not using social networks.

### 8.1.1 Malware

Malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware. In SNS the malware can use the personal data of the user to impersonate the user and send contagious messages to the user's online friends.

### 8.1.2 Phishing

Phishing is an attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

### 8.1.3 Spammers

Spammers are someone who makes the most of their advanced technological knowledge to place advertisements online without having to pay any costs. For example posting adverts to thousands of forums as regular users and regular forum posts without having to purchase advertising space.

### 8.1.4 Cross-site scripting (XSS)

It is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Their effect may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

### 8.1.5 Internet Fraud

An Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them; for example, by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software.

### 8.2 Modern Threats

Modern threats are mostly unique to the environment of SNS and which use the SNS infrastructure to endanger user privacy and security.

### 8.2.1 Click jacking

Click jacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms.

### 8.2.2 De-anonymization attacks

De-anonymization attacks use techniques such as tracking cookies, network topology, and user group memberships to uncover the user's real identity. It is possible for third parties to uncover SNS user identities by linking information leaked via social networking sites.

### 8.2.3 Face Recognition

SNS users upload millions and millions of photos everyday. These photos are publicly available to view and download. A biometric database can be created using these uploaded photos, which can then be used to identify SNS users without their consent.

### 8.2.4 Fake Profiles

Fake profiles are also referred to as Sybil or Social bots. Fake profiles can be used to harvest users' personal data from social networks. Friend requests are initiated to other users in the SNS, who accept the requests, the social bots can gather a user's private data which should be exposed only to the user's friends. Fake profiles can be used to initiate Sybil attacks, publish spam messages.

### 8.2.5 Identity Clone Attacks

Attackers duplicate a user's online presence either in the same network, or across different networks, to deceive the cloned user's friends into forming a trusting relationship with the cloned profile. The attacker can use this trust to collect personal information about the user's friends or to perform various types of online fraud.

### 8.2.6 Inference Attacks

Inference attacks are used to predict a user's personal, sensitive information such as religious affiliation or sexual orientation. These types of attacks can be implemented using data mining techniques combined with publicly available SNS data, such as network topology and data from users' friends.

### 8.2.7 Information Leakage

SNS users openly share and exchange information with their friends and other users in the network. SNS users willingly share sensitive information about themselves and other people, such as health related information and sobriety status. Leakage of sensitive and personal information may have negative implications for the social networks users.

### 8.2.8 Location Leakage

SNS users unknowingly share their locations by uploading photos and videos, which may be embedded with geotagging information about their current and past locations.

### 8.2.9 Socware

Socware entails fake and possibly damaging posts and messages from friends in OSNs. Socware may lure victims by offering false rewards to users who install socware-related malicious applications or visit socware websites. After the users have cruised the socware website or installed the relevant application, the installed socware sends fake messages on the user's behalf to the user's friends.

### 8.2.10 Combination Threats

Combination threats are threats where attackers can combine classic and modern threats to create a more sophisticated attack.

### 8.3 Threats Targeting Children

These threats specifically target children who use social networking sites.

### 8.3.1 Online Predators

Online Predators are defined as adult online users who seek to exploit vulnerable children or adolescents for sexual or other abusive purposes. Online Predators are sexual predators who use Information and Communications Technology and the Internet to locate, target and victimize minors.

### 8.3.2 Risky Behaviors

Potential risky behaviors of children may include direct online communication with strangers, use of chat rooms for interactions with strangers, sexually explicit talk with strangers, and giving private information and photos to strangers.

### 8.3.3 Cyber bullying

Cyber bullying has been defined by The National Crime Prevention Council as When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person [8].

## 9. Privacy Enhancing Technologies

Privacy Enhancing Technologies are generally designed to respect two important principles:

**-Data Minimization principle**
Data minimization principle states that "only the information necessary to complete a particular application should be disclosed"

**-Data Sovereignty principle**
Data Sovereignty principle states that "the data related to an individual belongs to him and that he should stay in control of how these data are used and for which purpose" [9].

## 10. Guidelines

The guidelines to enhance the privacy in SNSs are:

- Use two-factor authentication whenever possible
- Always look at the address bar of the website
- Do not add strangers to your friends list (even if stranger has many mutual friends, because reverse social engineering is a technique that hackers are using on Facebook)
- Use Anti-virus and anti-spyware applications on social media websites whenever possible.
- Always check the URL of a status before opening it.
- Do not use so many applications on the social networking websites or simply avoid. unnecessary applications.
- Be active in the security community to learn about the new threat.
- Keep your browser up to date because an out-dated browser is good victim.
- Keep all the necessary protection software up to date [10].

## 11. Conclusion

This paper presented privacy and privacy concerns. It also exposed the various threats to privacy and privacy enhancing technologies. SNSs are playing an important role in the Internet community today. Their future development hinges on their ability to deliver enjoyable services without undermining users' privacy. This article provides insights and clues that will lead to future improvements in SNS privacy.

## References:

1. Michael Beye, Arjan Jeckmans, Zekeriya Erkin, Pieter Hartel, Reginald Lagendijk and Qiang Tang, Literature Overview - Privacy in Online Social Networks.

2. Sharon Jayson, USA TODAY, Social media research raises privacy and ethics issues, http://www.usatoday.com/story/news/nation/2014/03/08/data-online-behavior-research/5781447/.

3. Social Networking Websites and Online Privacy – www.decima.com.

4. Shilei Zheng, , Kun Shi, , Zhu Zeng, Qiang Lu, The Exploration of Instrument of Users' Privacy Concerns of Social Network Service.

5. Blank, Bolsover & Dubois, A New Privacy Paradox: Young people and privacy on social network sites, Global Cyber Security Capacity Centre.

6. Adrienne Felt, David Evans, University of Virginia, Privacy Protection for Social Networking APIs.

7. RajneeshKaur Bedi, Nitinkumar Rajendra Gove, V.M. Wadhai ,Hippocratic Social Network ,2013 Fifth International Conference on Computational Aspects of Social Networks (CASoN).

8. Michael Fire et al., Online Social Networks: Threats and Solutions, IEEE Communication surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter 2014.

9. Esma Aïmeur, Sébastien Gambs, Ai Ho, Towards a Privacy-enhanced Social Networking Site, 2010 International, Reliability Conference on Availability and Security.

10. Social Media & Security Risk, posted in general security on September 4, 2012