www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 02, Issue 05, May 2022, pp : 408-413

e-ISSN : 2583-1062

Impact Factor : 2.205

HOW TO MAINTAIN PRIVACY IN SOCIAL MEDIA

Yash Yadav[*1], Sanjeev Soni[*2], Parth Joshi[*3]

[*1,2,3]Student, Computer Science, Dronacharya College Of Engineering, Gurgaon, Haryana, India.

ABSTRACT

Social networks have become a part of human life. Starting from sharing information like text, photos, messages, many have started share latest news, and news related pictures in the Media domain, question papers, assignments, and workshops in Education domain, online survey, marketing, and targeting customers in Business domain, and jokes, music, and videos in Entertainment domain. Because of its usage by Internet surfers in all possible ways, even wee would mention the social networking media as the current Internet culture. While enjoying the information sharing on Social Medias, yet it requires a great deal for security and privacy. The users' information that are to be kept undisclosed, should be made private.

Keywords: Social media; Privacy; Policy enforcement; Security.

1. INTRODUCTION

In recent years, Online Social Networks (OSNs) have seen significant growth and are receiving much attention in research. Social Networks have always been an important part of daily life, but now that more and more people are connected to the Internet, their online counterparts are fulfilling an increasingly important role. Aside from creating an actual network of social links, many OSNs allow their users to upload multimedia content, communicate in various ways and share many aspects of their lives. Because of the public nature of many social networks and the Internet itself, content can easily be disclosed to a wider audience than the user intended. Limited experience and awareness of users, as well as the lack of proper tools and design of the OSNs, do not help the situation. We feel that users are entitled to at least the same level of privacy in OSNs, that they enjoy in real-life interactions. Users should be able to trade some information for functionality without that information becoming available beyond the intended scope.

For example, a user of a self-help OSN like PatientsLikeMe, who suffers from a given medical condition might not want everyone to know about this, but at the same time the user would like to meet people with the same condition. This is the context of the Kindred Spirits project, and its aim is to provide users the ability to meet and interact with other (similar) people, while preserving their privacy. This paper aims to provide insight into privacy issues and needs faced by users of OSNs and their origins. The insights gained help plot a course for future work. To this end, we look at OSNs as they currently exist, the associated privacy risks, and existing research into solutions. The ultimate goal is to identify open topics in research through reflection on existing proposals.

2. ONLINE SOCIAL NETWORKS

Let us begin by framing the concept of Online Social Networks, and observe why OSNs are as widely used as they are today. This will help us understand the needs of OSN users, the environments they navigate, and potential threats as discussed in further sections.

2.1 Definition of OSNs

Boyd and Ellison's widely used definition captures the key elements of any OSN:

Definition 1. An OSN is a web-based service that allows individuals to:

1. construct a public or semi-public profile within the service,

2. articulate a list of other users with whom they share a connection,

3. view and traverse their list of connections and those made by others within the service.

The list of other users with whom a connection is shared is not limited to connections like friend (Facebook, MySpace) or relative (Geni), but also includes connections like follower (Twitter), professional (LinkedIn) or subscriber (YouTube).

2.2 The Rise of OSNs

The first OSN to see the light of day was Six Degrees in 1997. Six Degrees allowed users to create profiles, list and message their friends and traverse friends listings, thus fitting the definition above. Even though there were millions of users, users did not have that many direct friends and Six Degrees did not offer much functionality besides messaging. The website finally shut down in 2000. During and after this period other websites started adding OSN features to their existing content, essentially becoming OSNs, with various degrees of success. In the years that followed, new OSNs started from scratch and began to offer functionality beyond simply listing and browsing friends. Ryze and later LinkedIn tailored to professionals looking to exchange business contacts, while Friendster focussed on dating and finding new friends. Friendster became a mainstream OSN and was experiencing technical (performance and hardware) and social (fake profiles and friendship hoarding) difficulties because of its rapid growth. The technical

difficulties and actions to combat the social difficulties eventually led to users moving to other OSNs. Despite this, Friendster is still popular, particularly in the Phillipines, Indonesia and Myanmar. The popularity of Friendster encouraged the creation of other similar OSNs, like MySpace and Orkut. While Myspace has become popular among youth worldwide, Google's Orkut has attracted a predominantly Brazilian and Indian crowd. Aside 2 from these clearcut "social OSNs", a wide variety of niche OSNs have emerged, each catering to a particular taste. Adding the social structure of an OSN can often enrich the underlying services, making them more useful and attractive to users, or binding users to providers. Currently OSNs are an integral part of the internet.

2.3 Data in OSNs

Boyd and Ellison's definition already suggests that OSNs operate on two types of userrelated data: Profiles. A profile is tied to a user and is their representation to the outside world. Usually this is a self description, or the description of an alter-ego (pseudonym, avatar).

Connections. A connection exists between two users and can be of several types, like friend, colleague, fan, etc. A collection of connections can be represented by a graph. However, depending on the types of additional services the OSN offers, other forms of information related to users are often involved:

Messages. Messages in the broadest sense of the word. Any piece of data that is exchanged between a user and another user or a group of users, which may contain multi-media. This is the basis for additional OSN functionalities. Interaction between users has been recognized as a rich source of information on the underlying social network, even more so than friendship graphs.

Multi-media. Pieces of information that can be sent between users, but may also be uploaded to private or public data-spaces (e.g. photo album, blog, Facebook "Wall"). Examples are blog entries (text), photos (pictures), music or voice recordings (audio) and movie clips (video).

Tags. A tag can be defined as a keyword (meta-data) attached to content, by a user (either the uploader or other users). In Facebook terminology, 'tagging' refers to the specific case where a user identifies the people depicted in a photo, and tags the photo with their names, thus explicitly linking these people to the picture.

Groups. A collection of users. Usually groups also share some resource, attributes or privileges, for example: a collaborative document, common preferences or backgrounds, or access to a common space.

Behavioral information. Browsing history and actions undertaken by the user while performing tasks within the OSN. Benevenuto et al. note that this type of meta-data is particularly rich. Information such as preferences, friendships or even implicit data such as physical location can be inferred from it. Behavioral data is also found in traditional websites, although behavior there is not related to navigating a social network.

2.4 Proposed Methodology for Privacy issues in Social Media Sites

The sole objective of the study is to connect the quantitative system with a specific end goal to spuriously investigate the social information of the potential users and acquire the much needed details such as demographic data, temporal data, user profile etc., of the respondents. To augment this process, we had taken a survey system that will be thoroughly utilized and disseminated to over more than 200 social media users and the populace will be dictated by the non–probability testing strategy. Spiral testing and respondent-driven examining have additionally permits analysts to make gauges about the interpersonal organization joining the shrouded populace to solicit them on the protection from the current social network communities. Hence, this comprehensive study has focused more on privacy concerns hinges on the social networks and jolt out the privacy breaches effectively. We had identified some of the privacy concerns that the social users can undertake before they uses the social sites and embed their privacy setting on the site to prevent any breach of violation.

Predicting the behavior of social media users

This study goes for discovering the privacy and privacy in social network sites locales recognition among Social Media clients [6]. A specimen of 250 understudies was chosen haphazardly from distinctive piece of the world. A net of 185 polls were filled effectively and returned. Almost 78% of the respondents were males, while about 22% of them were females .On the other hand, roughly 72 of respondents were in the age bunch 20-35 years of age. Be that as it may, the quantity of respondents in the age gatherings "between 28-41 practically got 19% where different gatherings 50 or more is right around zero. Instructive level played a high effect subsequent to 58% are four year certification and graduate degrees are 21%. The years of utilizing Internet think about the commonality of interpersonal organization on the grounds that from those are utilizing the web for over 10 years are 56% and in the event that we connect the use with nature of SN it indicates 51 % for decently recognizable and 49% for extremely well known . Then again 90% of this study populace is utilizing Facebook and 36 % utilizing IslamTag and 62% twitter so this is leeway for us to think about Facebook protection model.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 02, Issue 05, May 2022, pp : 408-413

e-ISSN : 2583-1062

Impact Factor : 2.205

3. PRIVACY IN SOCIAL MEDIA

Making sure the OSN can perform desired behavior is one thing, but when sharing a wealth of (personal) data, one should also consider what undesired behavior might take place. In this section, we will look into privacy, its role in OSNs, and potential threats 6 to users' privacy. The word privacy has many subtly different meanings, ranging from personal privacy (which includes seclusion and bodily privacy) to information privacy, each with their own definition. Privacy on the Web in general revolves mostly around Information Privacy, as defined below in the IITF wording that Kang uses:

Information Privacy is "an individual's claim to control the terms under which personal information–information identifiable to the individual–is acquired, disclosed or used." In a Web2.0 setting, where users collaborate and share information, privacy of personal information becomes very relevant. In OSNs, users have a scope in mind when they upload information (see Palen and Dourish' classification below). Privacy involves keeping information in its intended scope. Such a scope is defined by the size of the audience (breadth), by extent of usage allowed (depth), and duration (lifetime). When information is moved beyond its intended scope (be it accidentally or maliciously), privacy is breached. A breach can occur when information is shared with a party for whom it was not intended (disclosure). It can also happen when information is abused for a different purpose than was intended, or when information is accessed after its intended lifetime. We also see this reflected in data protection laws, such as the Data Protection Act 1998 in the United Kingdom, where limitations are imposed to the extent and duration of use of personal data.

Provider-related Privacy Issues

A completely different type of privacy threat involves the relationship between the user and OSN provider, and in particular the trust that the user puts into the provider. This goes beyond user control of information, because the provider usually designed or configured the systems underlying the OSN. Thus the provider has full access to any userrelated data, including browsing behaviour and message logs. The associated threats are detailed below.

Data Retention

When posting information to an OSN it is often impossible or very difficult to remove that information. Facebook for example does not provide users with the means to delete their profile, and has actively blocked third-party software that attempts to remedy this. Even data that is apparently erased still resides elsewhere on the OSN, for example in backups, to be found by others. This is a violation of the 9 temporal boundary as information is available longer than intended. An example of this is given by Bonneau who tracked the availability of deleted photos. Also Facebook would like to store content forever.

OSN Employee Browsing Private Information

The OSN provider has full access to the data and an employee of the OSN provider might take advantage of this. This is in conflict with the implicit trust that is required in the OSN. All information supplied to the OSN is at risk in this issue, up to and including behavioral information. Interviews suggest that some Facebook employees can view user information and it is left to the company to police this.

Selling of Data

The wealth of information that is stored on the OSN, is likely to be of value to third parties and may be sold by the OSN. User preferences, behaviour and friendship connections can all be interesting for marketing purposes and research into social dynamics. Data sales can easily be in conflict with the implicit trust the user has in the OSN. One example of an OSN that provides user data to third parties is PatientsLikeMe. To quote their website:

"PatientsLikeMe offers pharmaceutical companies the opportunity to reach and learn from thousands of patients with chronic diseases. Follow their symptoms, treatments, outcomes and attitudes. Evaluate real-world safety and efficacy data, and conduct targeted clinical trial recruitment. These are just a few examples of how our portfolio of services drives value at each stage of the drug development process."

Targeted Marketing

Multiple pieces of information in the OSN can be combined to provide a high value profile of the user. This high value profile can then be used or exploited to present targeted marketing to the user. This again is a conflict of the implicit trust the OSN has, as information is used in a different manner than as intended by the user. An example of a company which uses OSN data for targeted marketing is Trust Fuse.

Trust Management and Issues

Protection is a precondition for online self-divulgence, yet self-revelation additionally diminishes privacy by expanding the measure of online data accessible to different clients; the connections between these builds appear to be affected by critical variables, for example, trust and control. Trust is characterized as the conviction that people, gatherings, or establishments can be trusted. It frequently has an opposing association with protection, if in light of the

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 02, Issue 05, May 2022, pp : 408-413

e-ISSN : 2583-1062

Impact Factor : 2.205

fact that individuals need to know data about others keeping in mind the end goal to trust them, which thusly has a beneficial outcome on online self-exposure. Then again, the advancement of trust in an online domain is unpredictable on the grounds that the online world is characterized as frail. This is the reason a few studies have concentrated on the inclination of individuals to unveil data on the premise of both trust and protection. An imperative build that can impact this mind boggling relationship is the apparent control over data. For instance, word check, things constructed particularly, and prepared raters are regularly used to quantify online self-divulgence, and adjustments of instruments assembled for up close and personal correspondence are utilized to assess online trust.

3.1. Privacy Setup on Social Networking Sites

Late research has investigated the relationship between the online revelation of individual data and privacy concerns and the high hazard identified with online ruptures of protection. It was also well suggested that privacy is a term that is hard to characterize; legitimately, it alludes to one side to be not to mention, yet it can likewise incorporate the privilege to choose the degree to which individual data is revealed, the privilege to focus at the point when, how, and what data can be imparted to others . Finding that one's own particular private data has been scattered internet, including humiliating photographs or features that are recovered through phishing tricks or deficient protection limitations, speaks to a genuine mental danger. On Facebook, the setting is liquid and flimsy, Senthil Kumar N. et al. / Procedia Computer Science which has imperative ramifications in regards to the administration of privacy on Facebook. Clients' impression of their gathering of people are frequently thought little of as far as both size and scope, and the protection administration settings are regularly entangled, futile, and demand particular assessments. Privacy dangers are regularly thought little of, while the social advantages emerging from the revelation of individual data are frequently overestimated. Besides, online ruptures of privacy are as often as possible thought to be a working's piece of Facebook, and solicitations for individual data don't stress clients. These attributes of privacy administration impact web unveiling conduct and clients view they could call their own self-revelation.

3.2 Summary

Because OSNs contain massive amounts of useful and interesting data about large numbers of users, they form an interesting target for third parties, both private and commercial. Either through browsing/spidering, hacking attacks or simple data-sales, this information could end up in the wrong hands. The fact that the users are not always the source of revenue for an OSN (in the case of advertisement revenue and data sales), can lead to conflicting interests for users and providers. Given the diverse and often extensive information available on OSNs, and the fact that threats may come from other users or even the service provider itself, the threats are myriad. Table 2 attempts to give a comprehensive overview. Concern in this table is high (), medium (•), or low (·). Despite the fact that prevention of these threats is no simple matter, many research areas in existing literature focus on alleviating some of the aforementioned threats

↓ Privacy concerns	Data types →	Profiles	Connections	Messages	Multi-media	Tags	Preferences	Groups	Behavioral information	Login credentials
User related	Stranger views private info	●	●	●	●	•	●	●	•	·
	Unable to hide info from specific friend / group	●	●	●	●	•	·	·	·	·
	Other users posting information about you	·	·	●	●	●	·	·	·	·
Provider related	Data retention	●	●	●	●	●	●	●	●	·
	OSN employee browsing private info	●	●	●	●	●	●	●	●	•
	Selling of data	●	●	●	●	·	●	·	●	·
	Targeted marketing	●	·	·	·	·	●	·	●	·

4. CONCLUSION

Within the Kindred Spirits project, matching of similar users and content recommendation are seen as central operations in OSN's. This makes "content recommendation" and "dating" OSNs the most relevant scenarios for the project. Main data types to protect from privacy-intrusions would thus include profiles, preferences, behavioural information and messages. The centeral operations to be performed on this data are clustering/matching, and filtering/search. The problems to be adressed by the Kindred Spirits project are not limited to the realm of "user-

related" threats. We feel that a user's privacy from the OSN service provider should also be guaranteed, and that this is in the interest of both users and service providers. The latter can benefit by improving their image for competitive advantage and avoiding problems related to data-protection laws

The technical solutions we have seen in focus on specific (categories of) problems. A solution to the general problem of lack of privacy in OSNs can be assumed to involve several of the aforementioned techniques. The identified topics in existing research relate to the Kindred Spirits project as follows:

Anonymization

Anonymization research is mainly useful after information has been supplied to the OSN. In the case of Kindred Spirits we aim to hide some information from the OSN. It seems that anonymization research does not match with Kindred Spirits.

Decentralization

In the Kindred Spirits project more control is given to the user and some information should be hidden from the OSN. Some degree of decentralization fits this picture, and may be used in our research.

Privacy settings and management

Kindred spirits should be able to find each other. In order to make this happen, users will have to specify which data they want to use for the matching process and also how important their privacy is in this process. In order to convey this, some form of privacy management is needed. Research into gradual and fine-grained privacy-management fits one of the central hypotheses of the Kindred Spirits project.

Encryption

In order to hide information from the OSN, while still making use of a central infrastructure, encryption is necessary.

Awareness, law and regulations

This field of research complements the Kindred Spirits project as it will work towards OSN users becoming more privacy-aware, and OSN service providers adopting a more serious attitude towards preservation of privacy. However this field is also outside the scope of the Kindred Spirits project. Considering the above, it seems natural for the research in the Kindred Spirits project to revolve around encryption and small scale decentralization, backed up by proper tools for managing privacy settings. The solutions should aim to protect profiles, preferences, behavioural information and messages, while still allowing the service provider to cluster or search the data.

In **conclusion**, the schemes and protocols developed in the Kindred Spirits project should facilitate (partial) hiding of user data from the OSN and other users through encryption, while maintaining the ability to find kindred spirits (matching between users) or provide media recommendations. When a match between users is found, further protocols should facilitate additional functionalities, such as gradual information disclosure, or exchanging recommendations in a privacy-friendly way

5. REFERENCES

[1] Dahlgren, P 2009, Media and political engagement: citizens, communication, and democracy, Cambridge University Press, New York.

[2] Della Porta, D & Mosca, L 2005, 'Global-net for global movements? A network of networks for a movement of movements', Journal of Public Policy, vol. no. 1, pp. 165–190.

[3] Eltantawy, N & Wiest, JB 2011, 'Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory', International Journal of Communication 5, pp. 1207-1224.

[4] Granqvist, Manne 2005, 'The information society: visions and realities in developing countries', in O Hemer & T Tufte (eds), Media and glocal change: rethinking communication for development, CLACSO, Nordicom, Buenos Aires, Göteborg, pp.285 – 296.

[5] Haenlein, M & Kaplan, MA 2010, 'Users of the world, unite! The challenges and opportunities of social media', Business Horizons, vol. 53, pp. 59-68.

[6] Hafferman, V 2011, 'The Digital Revolution'. La clé des Langue, viewed 21 September 2011, http://cle.ens-lyon.fr/93744078/0/fiche_pagelibre/

[7] Hartung, A 2011, 'Why Facebook beat MySpace', Forbes Online, viewed 26 September 2011, http://www.forbes.com/sites/adamhartung/2011/01/14/why-facebook-beat-myspace/

[8] Hinchcliffe, D 2006, 'The State of Web 2.0', Web Services Journal, viewed 27 September 2011, http://web2.wsj2.com/the_state_of_web_20.htm

[9] About US (2011), viewed 25 September 2011, http://tahrirdiaries.wordpress.com/about/

[10] Appadurai, A 1996, Modernity at large: cultural dimensions of globalization, University of Minnesota Press, Minneapolis.

[11] Bajarin, B 2011, 'Could What Happened to MySpace Happen to Facebook?', Time Online, viewed 20 September 2011, http://techland.time.com/2011/07/15/could-what-happened-to-myspace-happen-to-facebook/