ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Privacy and Privacy Nudges for OSNs: A Review

Ritu Gulia, Dr. Sapna Gambhir

Research Scholar, Department of Computer Engineering, YMCAUST, Faridabad, India

Associate Professor, Department of Computer Engineering, YMCAUST, Faridabad, India

ABSTRACT: Online Social networks are the hottest topic for everyone and also for researchers just because of its popularity. Online social network provide means to stay connected with your friends virtually. The privacy is one of the most important security concerns of the online social network. Privacy is basically when information is shared to wider audience than intended by the user. In this paper we discuss various privacy issues of the online social networks and their counter solutions to handle these issues. And most important solution privacy nudges are discussed and its various types, advantages, limitations, and future improvements are discussed.

KEYWORDS: Privacy, Nudges, OSN, Privacy Issues in OSN, Online disclosure, soft paternalism.

I. INTRODUCTION

In recent years, Online Social Networks (OSNs) have significant growth and receiving much attention in research. Social Networks have always been an important part of daily life, but now more and more people are connected to internet, their online counterparts are fulfilling an increasingly important role. Apart from creating the actual network of social links, many OSNs allows their users to upload multimedia content, communicate in various ways and share many aspects of their lives. Due to public nature of social networks, content can be easily disclosed to a wider audience than the user intended. This is the place where "Privacy" is needed. Privacy means the right to prevent ones personal information from being exposed to others. There are many issues related to privacy of OSN but also exist many counter solutions to handle these problems. To handle one these privacy issues of OSN is "PRIVACY NUDGE" new counter solution is introduced in OSN. Nudge can be defined as a way to provide gentle reminder to the user. In this paper, Privacy in OSN and its issues are discussed and existing solutions and new solution Privacy Nudge and its type's advantages and limitations are also discussed.

II. RELATED WORK

The rapid growth of the Online Social Network (OSN) is threatening the stability and security of the OSN users. Security of the OSN itself has many dimensions like authentication, integrity, and privacy. Privacy in the networks is one of the most important part of the security. Privacy in the OSN for an OSN user is important ingredient of security.

Boyd and Ellison's [1] defined OSN along with its key elements. They said "an OSN is a web-based service that allows individuals to:

- construct the public or semi-public profile within the service,
- articulate the 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".

Widely used OSNs are Facebook, Twitter, YouTube, and LinkedIn etc. In OSNs, Different names are used by different OSNs for shared connection viz. Shared connection is named as Friend in Facebook, follower in Twitter etc. Dictionary meaning of Privacy is "a state in which one is not observed or disturbed by other". The word privacy itself has many meaning varying from personal privacy to informational privacy. The privacy which is required in OSN is information privacy. Privacy on the web in general revolves mostly around *Information Privacy*. kang[2] defined information privacy as "an individual's claim to control the terms under which personal information- information identifiable to the individual - is acquired, disclosed, or used". In OSN, there are two types of information associated with the user's profile: explicit and implicit. Explicit information is the information stated by the user on purpose. For example user's phone number is added in its OSN profile provided intentionally for contact. Explicit information is not

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

necessarily accurate. Implicit information that can be inferred from user community based on explicit information e.g. a user is connected to many other users and most of them are stated favourite actor as *Johnny Depp* on their profile. It is therefore implied that user's favourite actor may be *Johnny Depp* it might not be correct. Implicit information is not always correct. In web 2.0 where users collaborate and share information with other users, privacy of personal information becomes very relevant. Privacy in OSN involves keeping the information in its intended scope of user. Such a scope can be defined by various parameters like by the size of audience, extent of usage allowed and duration (lifetime) etc. When the information is moved beyond its intended scope (accidentally or maliciously), privacy is compromised. In order to avoid this situation, Palen and Dourish[3] classify three privacy boundaries which when maintained by the users result in more security related to privacy. *Disclosure Boundary* manages the difference between public and private information (e.g. user profile contain two types of information public or private so information which user want to share with everyone is made public and the information which user want to hide from outside the OSN world is made private.). *Identity Boundary* manages the self representation with specific audience (e.g. there are many user community are present within the OSN so user can be part of any user community based on user interest .Suppose user join one community that community belongs to his or her college friends and join one more community which belongs to his or her office friends. So some part of information is not shared among these two communities like User College pictures is made public to user college community but not shown to his or her office user community.). Temporal Boundary manages the past actions with future expectations (because user's behaviour may change over time).

The reality of the OSNs is that data and identity of the user are closely related and often visible to large groups of people. This makes the privacy and information management difficult and give rise to privacy issues.

A. *Privacy Issues in OSNs*

On the basis of the information that user accesses, privacy issues are categorized in two main category [4,5,6]. One category that involves disclosure to other users relates to User Related Privacy issues. Other category originates from the provider and known as provider related issues. Fig. 1 shows various types of privacy issues are:

User Related Privacy Issues*:* Most of the time, privacy is breached by the fellow user or unregistered visitors. This may be intentional or accidental and can have serious consequences. Various Users related privacy issues are:

Unknown User Views Private Information: Due to lack of understanding or attention of the user towards privacy controls leads to disclosure of private information to wider audience than intended. Sometimes, users can falsely assume some of the information as private but in reality it is not. This can be due to the design flaws of the OSN and OSN service provider. Most of the time user is not aware of the privacy facility available to the user by the OSN provider for e.g. in Facebook, the privacy settings are not fine grained and the users have to explicitly apply these privacy settings. When the stranger views the private information of a user, this is a conflict with disclosure boundary. The user has lost the control over private information.

Unable to Hide Information from Specific Audience: Sometimes user wants to hide information from specific fellow user or group of friends. E.g. a user specified the reason of illness in the office but actually he is partying with his college friends. So, user did not want to share his party picture with office colleagues. In OSN world, it is not possible because anything goes online is viewed by all fellow user with whom they share connection. Most of the OSN provides various options for hiding information but not at such a fine grained level. The problems lead to identity boundary that users do not have control to act differently towards one user or group of user, than others.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

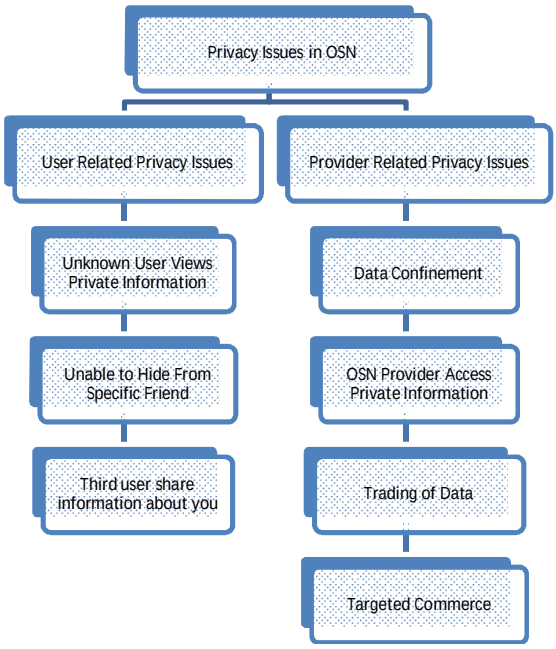

Fig. 1 Various Privacy Issues in OSN

Third User Sharing Information About You: User can control himself for posting some ill-legal information on the OSN but he or she can't stop his fellow users for the same. This sharing is possible because of some personal disputes or due to any wrong intention. This issue leads to disclosure boundary as the information is made more public than intended. The most important issue of this category is *cyber-Stalking* [7] which means "the use of the internet to stalk or harass an individual or group of individuals, or an organization. It may include making of false accusations or statements of fact, monitoring, making threats, identity theft, and solicitation of minors for sex or gathering information that may be used to harass".

Provider Related Privacy Issues*: This category of privacy issues* involves the relationship between the user and OSN provider. Provider is considered to be reliable and user trusts 100% on the provider. The provider can access both private and public information of the user. The associated threats are:

Data Confinement: Once a information is posted on OSN, it is often impossible or very difficult to remove that information e.g. Facebook provider does not provide facility to completely delete the profile of the user. Data which is once erased still resides either on provider's side or in the form of backups by other users. This is the violation of the "temporal boundary" as the information is available longer then intended.

OSN Provider Access Private Information: The OSN provider has full access to the data and its employees that might take the advantage of this .This is a conflict with the implicit trust that is required in the OSN.

Trading of Data: Wealth of the user's information can be of more valuable for third parties and may be sold by the OSN. User Preferences, behaviour and friendship connections can all be interesting for marketing and research purposes. Data sales can easily be in conflict with the implicit trust user has in OSN.

Targeted Commerce: 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 commerce to the user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

B.COUNTER SOLUTIONS OF PRIVACY ISSUES

Various methods to mitigate privacy issues are proposed by various researchers. The details of methods are:

Annonymization: This method that is used to publish the OSN data and protect user's privacy at the same time. Basic method of annonymization simply removes any identifying and identifiable information from data. The two main categories of annonymization techniques [7,8] one is cluster based and one is graph modification. These annonymization techniques are simple to implement and need to performed only once on a given snapshot of the OSN before sales to third parties.

Decentralization: In decentralized framework, an OSN user does not need to join any particular OSN service such as Facebook or MySpace. Instead, the user chooses a server which he/she trusts to host his own data such as his FOAF (Friend-of-a-friend) file, his activity log and his photo albums [17]. A user's FOAF file plays the central role in the decentralization framework. The FOAF specification provides a format for specifying "friends" relationships among people. Decentralization can happen to different degrees. A slight decentralization would gives user's a direct link to one another for chatting. In this way the chat data never passes through the server. An extreme case would be removing the OSN altogether and have all traffic takes place through the peer-to-peer network. A decentralized structure works strongly towards taking power away from the OSN provider, thus reducing the trust issue. Scalability in decentralized solutions is often good. The biggest problem with the decentralization is the technical feasibility of the framework.

Privacy Settings and Management: Users need to be confirmed about the consequences of their various information publication and their activities; need to know which part of their information is accessible and for whom; need have some facilities to control the way that people can access their information; and need to get all the requirements in a simple and understandable way that does not need a lot of time and effort. Privacy policies should be unambiguous short and simply understandable [15]. This is the first step of helping users towards their privacy protection. Accepting privacy policy agreement, there are some flexible privacy settings that could be adjusted and help the user to specify the way their information is accessible [16]. Since it is difficult for the average user to adjust these fine grained and detailed settings, some research has been done in this direction of helping users.

Encryption: Encryption can be used as a tool to provide confidentiality and integrity. Depending on how encryption is applied this can mean protection from unauthorized user or the service provider. It can be coupled with either decentralization or privacy setting and management. Lucas and Borisov [14] proposed the method to encrypt the certain part of the user's profile using public key cryptography. Keys are derived from user supplied passwords in order to maintain access flexibility's potential problem with this approach is resulting low entropy of keys. The advantage of this cryptographic approach is that this solves many privacy issues if used properly.

*Privacy Nudges***:** Privacy nudges are new solution for the privacy issues of OSN. The firstly privacy nudges are developed for Facebook. Nudges provides a gentle reminder to the user for a particular action. For example if an OSN user post something bad related to his fellow user than nudge can't force the user not to post but provide a gentle reminder to the user that it is wrong. Nudges are needed by the OSN in order to save the OSN user from wrong consequences of the internet sharing. A large portion of the OSN user regret over internet sharing because sometime user post under the influence of alcohol, post something related to politics which is wrong etc. these actions can damage the reputation of the user after which user regret. So in order to save the user nudges are helpful.

III. PRIVACY NUDGES FOR OSN

Privacy nudges are the applications of the soft paternalism. Dictionary meaning of Paternalism is "*the behaviour by a person, organization or state, which limits some person or group's liberty or autonomy for their own good*". The *soft paternalism* is also known as *asymmetric paternalism*. Thaler and Sustein[9] defined the soft paternalism as "*it tries to influence the choices in a way that will make chooser a better, as judged by themselves*". From the concept of the soft paternalism they defined the nudge. The dictionary meaning of the nudge is to provide gentle reminder to the user. So they defined nudge as "*any aspect of the choice architecture that alters' people behaviour in a predictable way without forbidding any options or significantly changing their economic incentives*". For example if user post something under the influence of heat(angry) then nudge can't stop him posting the post but rather than nudge the user by providing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

reminder to the user again that it is wrong. In the offline world it is possible to tailor [10] our comments, hiding our gestures or actions from group of people. But in online world if something once shared it is seen by all. If OSN user wants to hiding something form specific audience then this facility is not provided in the OSN. The effect of this is that user stops sharing something related to him. User finds its identity and disclosure boundary are compromised so it stops sharing in the OSN. This will lead to "*context collapse*" [11].In order to overcome from context collapse OSN provider should provide proper privacy to the OSN user. If privacy is breaches in the OSN then it consequences very dangerous.

The consequences of privacy "breaches" in OSN may range from simple embarrassment to stalking, identity theft or damaged reputations [1]. Recently Wang.et.al offered empirical evidence how Facebook disclosures led to negative outcomes including damaged personal relationships or problems at work place [11]. So in order to deal with this situation soft paternalism concept is studied and nudge is created.

A. *TYPES OF PRIVACY NUDGES*

Privacy nudges for OSN are firstly discussed in paper [12].They developed the three privacy nudges for OSN Facebook. Reason for opting Facebook is its popularity and complexity of the privacy issues associated with it. Different types of Nudges developed on some particular action are:

Picture Nudge: Picture Nudge is basically developed to nudge the user regarding the potential audience of his post. This nudge displays the five profile picture randomly selected from the pool of the people who can see the user post. They may be user friends or not. Seeing these profile picture user get the hint of the people with who can see this post. As a result of this nudge user can cancel the post just because it has been seen by the audience with whom user did not want to share his post. This nudge also help user to pay attention towards his privacy settings.

Timer Nudge: This nudge add delay to the actual post time. As user clicks on post button to share something then this nudge add delay of 10 seconds and gives time to the user to check or review the content of the post and gives the options to edit or cancel the post. If user finds its wrong then user can change or cancel the post. As the time reaches to 3 seconds left then again nudge the user at this time one more option is available post it now. If user finds the post correct than user can post it immediately without any delay. The main work of this nudge is to provide time to the user before posting. This nudge will be helpful when user is angry or sad.

Sentiment Nudge: This nudge is very important among all nudges. This nudge provide immediate feedback on the content shared by the user and add delay to the post. Suppose if user post something on his wall as user clicks on post button this nudge analyse the content word-by-word. This is done by using the AFINN-111 module which contains a list of 2500 words along with their rating. Positive words are given rating in the range 1 to 5. Neutral words are given 0.Negative words are given rating in the range -1 to -5.Using this module sentiment of the post is analysed and nudge the user regarding that this post is perceived as positive post or negative post. If the post is perceived as negative post then delays is added and option of edit, cancel or post now are available. This nudge is effective among all because it provide immediate feedback. This nudge does not understand the context of the post leads to wrong nudging.

B. *ADVANTAGES OF PRIVACY NUDGES*

The objective of the privacy nudges was to help users from making online disclosure for which they later regret. Nudges encouraged users to reflect on their post and audience. Advantages of the privacy nudges are:

Stop and Think: Timer and sentiment nudge add delay to the actual post. This delay will give time to the user to think about the post content and analyse it properly. If found something wrong then have sufficient time to correct it. It help user to avoid regrettable post. But this benefit comes at the cost of the delay.

Content Feedback: Sentiment nudge helps make users more aware of how others might perceive their post, since past research has found that posts are perceived as negative or contain sensitive topics are regretted.

Attention to Audience: Research has found that users often forget who are their friends on Facebook and have trouble in understanding their privacy settings. This feature is positively accepted by privacy nudge and seemed positive effect on

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

the user. Profile nudge basically gives hint to the user to pay attention to the audience. Showing profile pictures of the people who can see the post encourage users to be more aware of or more cautious about their posts.

C. *LIMITATIONS OF PRIVACY NUDGES:*

Nudges helps users to think about their post before actually posted. Currently, nudges have many limitations which can be the area of many researches. Limitation faced by OSN user while using nudges:

- Nudges are found irritating by the user because it applied on each post whether the post is negative or positive impact on the audience.
- Less effective.
- Algorithm used for finding the profile picture is not effective.
- Sentiment Nudge does not understand the context of the post [13].
- Sentiment Nudge is only limited to text only if user post other than text like video, image or other multimedia data sentiment nudge fails to nudge user.
- Timer nudge causes delay i.e. benefits of the timer nudge comes at the cost of the delay.
- Not interactive.

IV. CHALLENGING ISSUES IN PRIVACY NUDGES

The concept of nudge is very beneficial not only for the OSN but for other domains also. But there exist many challenging issues with the privacy nudges. For example, suppose user post images in the OSN rather than text than sentiment nudge not able to nudge user because sentiment nudge does not support image and in the OSN world multimedia data is more used than simple text. So there is a need to optimize the sentiment nudge. Another issue, suppose user comment on some political issues in taunting way which is considered in positive way by the audience but sentiment nudge gives output to the user as this post gives negative impact to the audience needs to modify. So this issue is that sentiment nudge does not understand the context of the post. So the main issue with the sentiment nudge is lack of context understanding and does not support multimedia data. Timer nudge causes the lot of delay in the post submission so needs to be reduced. All these issues need to be resolved for better result of nudges.

V. CONCLUSION

Privacy Nudges are designed using the concept of soft paternalism and choice of architecture. They provide visual cues about the audience, time delays, and content feedback. Privacy Nudges could be a powerful mechanism to discourage unintended disclosures in social network that may lead to regret. On analysis it was found that picture and sentiment nudge is more useful as compared to others. Nudges are the generalized concept so it can be applicable to other domains also. There is lot of space for improvement in the existing nudge and also lots of new nudge can also be created on different action of the OSN user. Existing nudge can be improved like making them interactive ,understand the context of the user data, support for multimedia content like image, video etc., reduce the delay time of the timer nudge etc. Finally, it was found that privacy nudging approach encourage other researchers to explore the rich design space of nudging to protect people privacy.

REFERENCES

1. D.Boyd and N.B.Ellison , ' Social Netwok Sites :definition ,history and scholarship', Proceedings of the Jounral of Computer- mediated Communication,Vol. 13(1), pp. 210-230(2007).
2. J.Kang ,'Information privacy in cyberspace transactions',Proceedings of the Jounral Standford Law Review,Vol 50(4),pp.1193-1294(1998).
3. L.Palen and P.Dourish, 'Unpacking "privacy" for a networked world'.In CHI '03 Proceedings of the SIGCHI confrence on human factors in computing systems, pp.129-136(2003).
4. J.Anderson ,C.Daz ,J.Bonneau, and F.Stajano' Privacy-enabling social networking over untrusted networks'.In J.Crowcroft and B.Krishanmurthy, editors WOSN,pp 1-6 (2009).
5. S.Guha,K.Tang and P.Francsis,' Noyb:Privacy in Online Social Networks'.In Proceedings of the first workshop on online social network ,pp 49-54(2008).
6. A.Tootoonchian,S.Saroiu,Y.Ganjali,and A.Wolman, ' Lockr:better privacy for social networks.In CoNEXT '09': In the Proceedings of the 5th international confrence on Emerging networking experiments and technologies,pp 169-180(2009).
7. B.Zhou ,J.Pie and W.Luk., ' A breif Survey on annonymization techniques for privacy preserving publishing of Social Network Data'.In Proceddings of Special Interest group on knowledge discovery and data mining Explorations. Vol 10(2),pp12-22(2008).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

8. L.Backstrom,C.Dwork, and J.Kleinberg, 'Wherefore art thou r3579x?: anonymized social networks , hidden patterns, and structural steganography'.In WWW'07 Proceedings of the 16th international confrence on world wide web, pp181-190(2007).
9. R.H.Thaler and C.R.Sustein,'Nudge:improving decisions about health,wealth,and happiness' edition 1.Yale university Press(2008).
10. E.Goffman, 'The presentation of self in everdaylife' Anchor 1(1959).
11. Y.Wang ,S.Komanduri,P.G.Leon ,G.Norcie,A.Acquisti,and L.F Cranor, 'I regretted the minute I pressed share: A qualitative study of regrets on Facebook'.In Proceedings of the 7th Symposium on Usable privacy and security(2011).
12. Y.Wang ,K.Scott,P.G.Leon ,G.Norcie,A.Acquisti,and L.F Cranor, 'Privacy Nudges for Social Media:An Exploratory Study of Facebook'.In Proceedings of Second International workshop on Privacy and Security in Online Social Media(2013).
13. J.Weizenbaum,'ELIZA – a computer program for the study of natural language communication between man and machine '.In Proceedings Commun Vol 9(1),pp. 36-45(1966).
14. M.M.Lucas and N.Boriso,'Flybynight:mitigating the privacy risks of social Networking'.In Proceedings of the 7th ACM workshop on privacy in the elctronic society(WPES),pp 1-8(2008).
15. E.A.Baatarjav,R.Dantu,and S.Phithakkitnukoon,'Privacy Management for Facebook'.In Proceedings of International Confrence on Information Systems Security,Vol 5352,pp-273-286(2008).
16. R.Leenes,'Context is everything – Sociality and Privacy in online social network sites'.Vol 320, pp 48-65(2010).
17. CA.Yeung,I.Liccardi,K.lu,T.B.Lee and O.Senevirtante,'Decentralization:The Future Of Online Social Networking'(2006).