Designing User Centric Online Privacy

Puneet Kaur
Aalto School of Science and Technology
pkaur@cc.hut.fi

Abstract

The rapid deployment of the Internet services such as social networking services has provided a great convenience to the people. On one hand, these services have made human life much easier but on other hand privacy exposure poses a grave threat to user's identity due to the inherent handling of the personal data. User's privacy must be protected and the access to the personal information should be given in accordance to the user selected privacy settings. Privacy issues raised by the usage of social networking sites has attracted more and more attention over the years. The aim of the paper is to survey and compare various mechanisms of achieving user centric privacy control in social networking services and challenges faced by them. The paper suggests few guidelines for modeling user-centric on-line privacy. It also discusses a framework for designing user-centered online privacy which targets at minimizing the burden on the users.

1 Introduction

Internet through the means of social networking sites (SNS) has provided opportunity to the users with various backgrounds and technical skills to communicate, interact and share their personal or professional information with others in the on-line environment. The popularity of SNS like Facebook, MySpace, LinkedIn etc has been increasing rapidly [4] [2]. More than 500 million active users spending over 700 billion minutes on Facebook every month serves to be a typical instance for showing the ever increasing use of SNS [1]. Cutillo et al and Boyd et al [4], have defined SNS comprehensively as the *web based services that allows individuals to (1) construct a public or semipublic profile within a bounded system, (2) articulate the list of other users with whom they share a connection, (3) view and traverse their list of connections and those made by others in the system, (4) communicate with other users through direct, sometimes instant message exchanges or annotation of profiles and, (5) enable a wealth to third party application by featuring advanced interactions ranging from simple poking of other members to support for special interest groups and exchange of virtual gifts*. Just like a coin, SNS also has two sides associated with it. On one hand, SNS has good side affiliated to it, as the original idea behind the usage of SNS was to provide the users with the opportunity to socialize, interact and communicate with friends, relatives and other people with similar interests across the geographical boundaries. But, at the same time it also brought along with it several privacy and security threats. Since the success of SNS depends on the number of members registered with them, due to which major efforts are being spent on the making them more attractive thus, leaving the privacy and security concerns behind the corner [10]. Good objectives of SNS were ruined when people started misusing it. SNS enables people to interact with several applications and other users on the network. During these interactions people intentionally or unintentionally reveal some private information about themselves [13]. The basic problem in this situation is that the user's information can be viewed or gathered without their consent and often without their knowledge, which makes the context more risky and untrustworthy [11]. So, measures need to be taken to prevent user's personal information from being eroded. The increased level of misuse of personal information, paved the way for the emergence of various privacy policies [9]. Privacy policy can be defined as the document that aims at helping the users in understanding and learning what the organizations are offering in the name of privacy. It informs its users about privacy settings are available to them that could help in controlling their privacy exposure in on-line environment. Privacy settings can be defined as the actual guardians of the users' privacy. They are the actual tools which empower the users to manage their privacy exposure in the on-line conditions. Some of the common privacy settings can be related to *profile privacy* (who can view users' profile and their personal information), *application privacy* (what user information is being shared with the applications that they install) and *search privacy* (who can search the user) [1]. Moreover, there could be various attacks in the SNS against the privacy of the users. Cutilli et al [4] have listed several attacks against the privacy of the users such as identity theft, profile cloning, profile porting, face recognition, communication tracking etc. The rest of the paper has been organized as follows. Section 2 presents some of the related relevant work to the area under investigation.Various privacy control mechanisms have been elaborated in Section 3 which further discusses about their differences and challenges faced by them. Section 4 deals with user-centric privacy model along with the guidelines for designing user-centric privacy. Finally, the paper concludes with the discussion in Section 5.

2 Related Work

Feng Zhu [14] created an experimental design to understand different issues related to identity exposure, user's actions, and attitude related to privacy and identity concerns. Eldin

[1] Facebook Statistics,www.facebook.com/press/info.php?statistics

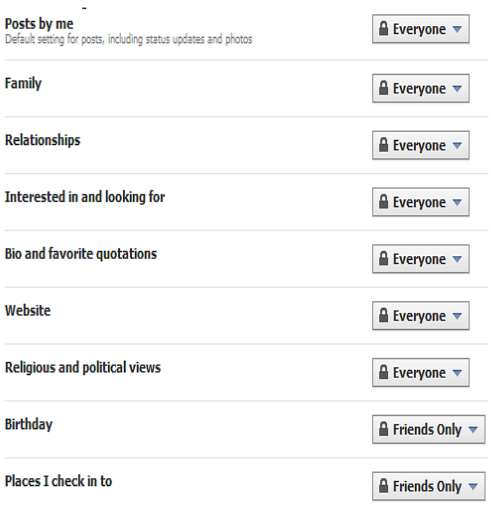

Figure 1: Default privacy settings

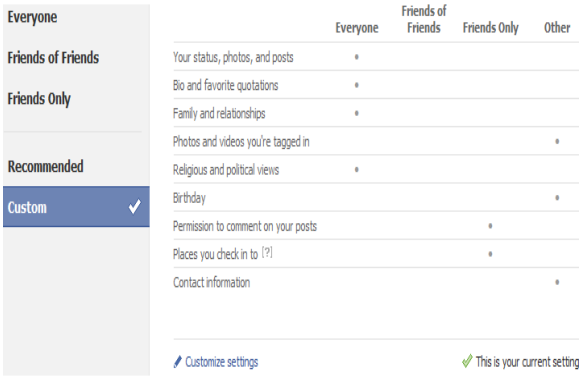

Figure 2: Customized privacy settings

[6] proposed a privacy architecture which allows a user to automatically control the privacy exposure based on fuzzy reasoning while the user can also define its own privacy preferences. The results were compared for automatic privacy control,manual handling and hybrid version of automatic and manual methods. Garcia [8] focused on an integrative approach to privacy that takes into consideration legal, technological as well as user centric deigns aspects. Based on all the above parameters Garcia et al come up with an integrative solution to on-line privacy referred called User Centric Privacy Framework (UPF). Cutillo [3] coined the idea of preserving privacy in social networks through decentralization. A combination of anonymity, Trust management and peer to peer system is advocated to achieve the desired results. They also reflect upon the three tier architecture of SNS having social network, application and communication/transport layers at its core. Saleh [12] has proposed a model for user's privacy preferences which incorporates user activity as key to decide and take actions. The proposed approach follows case based reasoning for relating the current activities with the past activities thus forming an intuitive understanding for making the desired privacy preferences.

3 Different types of Privacy Control Mechanisms

There are mainly four different types of privacy settings. They can be defined for-example by the service, individually by the user, both by user and service or even dynamically by the context factors such as recommendation, reputation and particular user behavior.

1. **Default privacy** -The default privacy settings of SNS can be defined as the settings which provide the users with the pre-configured privacy settings. An example of the default privacy settings has been presented through Figure 1. It shows pre-configured privacy settings of Facebook where by default users' posts including their status updates, photos, family information, relationship status, interests and likes etc are being shared with everyone on the network. On the contrary, it would have been better or in welfare of the users if all the above settings are only shared with their friends by default. The default privacy settings have a convincing impression on the popularity of the SNS. Majority of the users keep their default settings as it is hence it is important to provide convincing default privacy settings that can serve the masses or generic population of the users [1]. Hence, for the actual success of any SNS it is very important that their pre-configured privacy settings are very strong in protecting their users' privacy in the online environment.

2. **Customizable privacy** - Another kind of privacy settings termed as customizable privacy settings also exist. The customizable privacy settings also referred as custom settings can be defined as the ones that allow users to set or configure their privacy settings themselves according to their requirements. The privacy settings of the SNS should provide freedom and flexibility to their users in making their privacy settings. This facility provides complete control in the hands of the users so it might lead to trust generation between the users and the particular SNS that they are using. Figure 2 shows the example of Facebook which allows its users to customize or personalize their privacy settings when required by the users.

3. **Privacy settings based on User Privacy Policies (UPP)**- UPP based privacy settings are implemented on P3P platform (The Platform for Privacy Preferences Project). They take into consideration not only the importance of data that is being disclosed but also the user with whom the data is being shared. It allows the users to declare their privacy settings in the form of a contract to the intended parties namely; other users, third parties applications, websites etc and SNS's service providers [1]. The users are provided with the flexibility to build their UPP which consists of specifying a single or multiple elements. Each element consists of the specifications about its owner, the receiver and the list of access

rights. It also allows the users to customize the tracking options as well from no possibility of being tracked to no restrictions at all. Though these settings seem to be quite useful and flexible but they demands a lot of time and effort from their users which might serve to be one of the biggest hindrance in the adoption of this approach of controlling privacy exposure.

4. **Adaptive privacy** -The adaptive privacy settings can be defined as the one that can be extracted automatically using techniques like machine learning. The main objective behind having such dynamic or contextual approach is that the previously discussed approaches to privacy are rigid and could fail to be applicable as the context of SNS is implicit, ever changing, and not a-prior known to the service provider, requires the user to manually label all interactions or authorize them individually becomes a usability nightmare [5]. Some of the approaches to adaptive privacy settings are discussed below:

   - **Sub-graph based approach**: Danezis [5] has proposed a sub-graph based approach that could be used to implement adaptive privacy settings by extracting the context in a transparent and friendly manner. The context can be defined as the set of contacts of a user, that are closely related to each other, in such a way, that one would expect information about the user's interactions with one of them to become known to the others, independent of the SNS [5].

     In this approach a set of possible contexts are automatically extracted through the means of the sub-graph around a particular user using greedy algorithm. The main reason for using the sub-graph based approach is to ensure a privacy friendly and transparent context extraction. The sub-graphs used in the technique are large groups having moderate density consisting of number of high density but small graphs. One of the extracted contexts can then be assigned to the interactions automatically or with minimal user help. Finally, based on the assigned context the default visibility for that context can be assigned to the interaction. The usefulness of this approach depends solely on the accuracy of the extracted contexts and users tendency to accept them. But, usage of this scheme is not appropriate as the concept of using extracted contexts can be visualized as removing user's autonomy.[7]. This is due to the fact that extracted contexts reflect users' preferences which might lead to several privacy and security threats and implications for them.

   - **Implicit rules based approach**: Fang et al [7] has proposed a generic privacy preference framework based on the implicit set of rules gathered from the users themselves and their visible profile data for automatically configuring their privacy settings. In order to automatically extract accurate privacy settings, an active learning technique referred as uncertainty sampling is being used. The generic architecture following uncertainty sampling and working of the privacy preference framework has been depicted through the Figure 3. The proposed privacy preference predicting framework has high accuracy rate, incorporates the concept of graceful degradation, and is scalable. The basic wizard is also quite simple to use for typical (non-Technical) users to use. But, the advanced technical users may complain that it does not allow them to view or directly manipulate the resulting privacy-preference model [5].

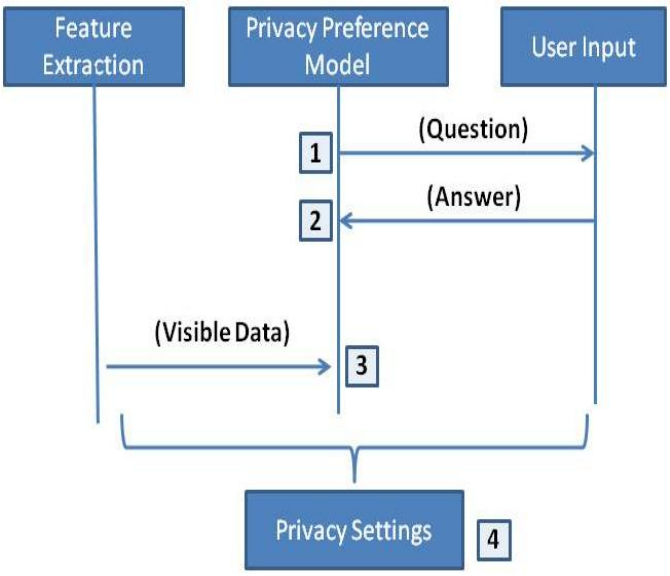

Figure 3: Implicit rule based adaptive privacy

3.1 Problems and Challenges

The privacy policies and settings provided by various SNS face several challenges and problems. Various challenges faced by SNS are:

1. **Usability**- One of the main challenges faced by the privacy policies and settings is their usability. The privacy policies require the users to perform various privacy settings in order to control their privacy exposure in the on-line environment. However, the privacy policies providing information about the available privacy settings might be confusing and difficult for the users to not only grasp them but also set them. This can be substantiated by taking into consideration the case of Facebook. Facebook offers privacy to its users through the means of 50 settings that make up a total of 170 options [2]. It offers its users to make privacy settings related to: their personal and contact information, friends, tags, connections, applications and websites, searching and third party advertisements. The infrastructure for making the privacy settings is quite wide. The survey conducted by Aimeur et al [1] reveals that it is not always clear to the user how to use privacy settings to

[2] New York Times, www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html

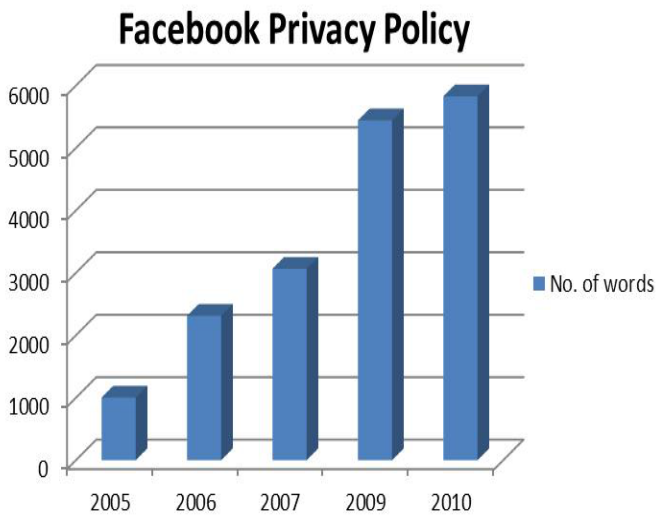

Figure 4: Increasing number of words in privacy policy

Figure 5: Users have to share their information to use the service

block unwanted people or prevent unauthorized ones from accessing his profile.

2. **Length of Privacy Policies**- The other major problem with the privacy policies is their length. The privacy policies help the users in understanding and learning what settings are being provided to the users by the concerned SNS for controlling their privacy exposure. But, the policies of the major SNS are quite long which might affects user's willingness to go through them. For example the number of the words in the Facebook's privacy policy has been growing ever since last five years (c.f. Figure 4). The length of the privacy policies of the major SNS has been shown in the Table1.

SNS	Number of words
Facebook	5823
Twitter	1254
Orkut	1519
MySpace	2740
hi5	2222
Friendster	1982
LinkedIn	6278
Bebo	2797

Table 1: Comparison of Privacy policy word length

3. **Lack of Awareness**- Majority of the users join SNS with the aim of being connected with their family and friends while privacy policies and settings remain secondary things for them. Other problem with the privacy settings is that the users might not know how to use them due to which the usage of privacy settings is not able to bring the desired level of protection to the users. Sometimes the privacy policies are revealed to the users when they are registering for the service. In order to continue using the service they need to accept certain terms and conditions. Figure 5 presents one such scenario from Facebook where the user has to make a trade-off between the information that the user has to share in order to use the service. However, SNS are making efforts in this direction by making their privacy policy explicitly discuss how the various controls work and how users could set them.

4. **Lack of Visibility**- Many SNS regularly update their privacy policies and available settings but do not inform their users explicitly that they have been updated. In addition, most of these sites do not even inform their users the consequences of making a particular privacy control setting.

5. **Designing Privacy Settings**- Designing the privacy settings is also a challenge in itself. This is particularly due to the fact that the privacy settings being designed are meant to be used by global user-base. The global user-base consists of users having different backgrounds, culture, skill set, etc which makes them different from each other. Most of them have different expectations from the privacy settings depending on their usage and needs. It is quite a big task for the SNS to come up with some privacy policies and settings that could satisfy all their users.

3.2 Comparison of various privacy control mechanisms

The differences between various mechanisms available for preserving privacy in the on-line environment have been presented in Table 2 and Table 3. The differences between various mechanisms have been discussed based on their characteristic features. They have been detailed below:

1. **Usable**- The feature of being usable is not applicable (NA) to the default privacy settings as the user does not need to set them at all. Whenever the users joins any SNS then they are provided with the pre-configured settings by default. However, in the case of customizable privacy settings the usability depends on the service that the users are using. The details related to this have already been discussed in case of the privacy settings of popular SNS Facebook. UPP is not usable as the users have to specify the receiver's names and the access rights that they want to give to the others users of SNS by themselves which requires a lot of time and effort. Adaptive privacy settings such as sub-graph and implicit rule based are usable in the sense that the minimal or no user effort is required. Moreover, implicit rule based settings follows the principle of graceful degradation which means that users can any time refuse giving their input.

2. **Required time and effort**- There is no time and effort required (NA) in the case of default privacy settings as the users get them pre-configured by the particular SNS that they wish to use. However, the time and effort requirements are quite high in the case of customized and UPP as the users themselves make their privacy settings. But, again in the case of adaptive privacy settings users' effort is low as minimal or no user effort is required and they also have the option to opt out at any time they want.

3. **Effectiveness**- The effectiveness in the case of default settings depends on the pre-configured settings provided by default. For example: the default privacy settings in the case of Facebook are not effective as they lead to sharing of users' posts, status updates and photos etc to everyone on the network (c.f. Figure 1). In the case of customized privacy settings effectiveness depends on the skills and the background of the users. Even in the case of sub-graph based approach, the effectiveness depends on how accurately the contexts are extracted. But, UPP and implicit rule based approaches are quite effective in terms of the privacy they provide.

4. **User Control**-The user has no control at all in the case of default as they are getting these settings automatically. In the case of UPP and customized privacy settings users have complete control over their privacy. But, in the case of adaptive privacy setting uses exercise indirect control on their privacy settings.

Feature	Default	Custom	UPP
Usable	NA	Depends	No
Time-Effort	NA	High	High
Effectiveness	Depends	Depends	Yes
User Control	No Control	Depends	Complete

Table 2: Comparison between Default, Custom and UPP

Feature	Sub Graph	Implicit Rule
Usable	Yes	Yes
Time-Effort	Low	Low
Effectiveness	Depends	Yes
User Control	Indirect	Indirect

Table 3: Comparison between Sub Graph and Implicit Rule

4 Design

Privacy policies and settings are one of the means to model on-line privacy where default privacy settings make the things easy for a layman while customizable privacy settings and UPP based settings facilitates the users who can and want to manage their privacy by themselves. On the other hand, adaptive privacy settings automatically provides the privacy settings to the users with their minimal effort. As the privacy policies and settings are being designed and intended to be used by the users of SNS so they should always be modeled keeping them in mind. The privacy policies and settings modeled from the user's point of view together are responsible for generating the *user-centric privacy model*. There are several goals of achieving user centric privacy control like; transparent gathering of personal information and provision of enough choices to the users so that anyone can protect their privacy. On-line privacy modeling should be contextual and dynamic so that they satisfy changing needs of the users. The system should identify various aspects of the identity exposure such as privacy concerns, identities and user exposure behavior[14]. There are some guidelines for designing user centric privacy model and some of them have been discussed in following Section 4.1.

4.1 Guidelines for User centric privacy model

1. **Enhance usability**- The privacy policies and settings of the SNS should allow their users to have complete control over the information they are sharing. SNS should ensure that the infrastructure in terms of available options should not be too wide such that it becomes difficult for the users to follow them. In order to achieve this objective, the SNS should ensure that they allow their users to make most of their privacy settings with minimum number of clicks.

2. **Concise privacy policies**- The length of privacy policies should also be neither too large nor too small. They should neither be too small that they do not provide users with the required information. On the other hand, they should even not be so long that the users feel reluctant to go through them. These policies are quite important for the users to know as they inform the users about the general privacy statement of any SNS. To the best of our knowledge there has been no such studies that discusses about what should be the optimum length of the privacy policies.

3. **Upgrade awareness level**- All the SNS should make sure that they update their users in case of any changes or update in their privacy policies and settings. One of the ways of doing this could be making it appear

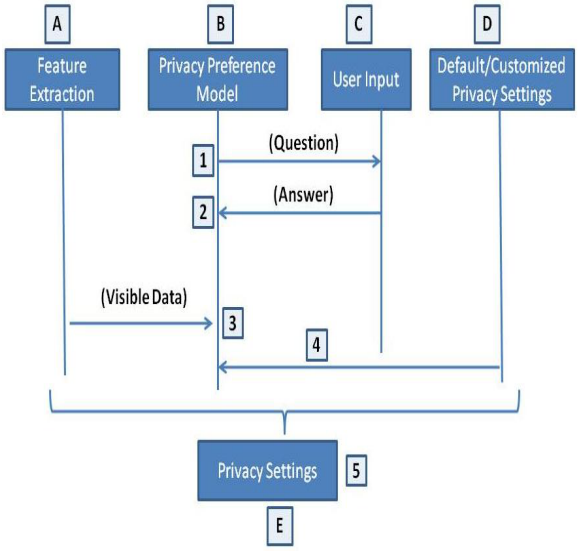

Figure 6: User Centric Privacy Model

as a general note to their users when they sign in after the changes have been made. This timely updating and intimation of the users will help in strengthening the trust and overall relationship between the SNS and their users.

4. **Increase visibility**- SNS should also make visible the impact of the privacy settings to their users. This can be done by making the users have a preview of the privacy settings. One of the ways of doing could be prompting the users with a dialog box asking them for permission whenever some new privacy settings have been generated or needs to be done. This has been discussed later in more details in Section 5.

5. **Design acceptable privacy settings**- The privacy settings should be a combination of three privacy control mechanisms -Default, Customizable and Adaptive. The next Section 4.2 presents User Centric privacy policy model.

4.2 User Centric Privacy Model

Based on all the studied approaches we suggest a user-centric privacy preserving model that will automatically generate the privacy settings for the user. The architecture for user-centric privacy preserving model has been shown in Figure 6.

The proposed user centric framework has been discussed below:

1. A (Feature Extraction)- will provide input based on the visible data on the user profile.

2. C (User) - will provide input to the system by answering questions put forward by the system.

3. D (Default/Customized Privacy settings) - will be fed into the privacy preference framework. This is also relevant as the user might already be using some privacy settings may be default or customized.

4. B (Privacy Preference Model) - takes all the inputs from A, C and D. Based on these inputs it proposes the automated privacy settings for the users.

5. E (Privacy Settings) - are the final generated privacy settings based on the various inputs provided to the privacy preference model.

Our model is the modification of the implicit rule based approach [7]. The proposed modifications take into account the privacy guidelines that have been discussed in Section 4.1. The applicability of the approach is decided by the users when they start using SNS by making their account. Whenever the user joins the SNS service the user is prompted with the question asking them to choose between:

1. I am technical user and would like to make my own privacy settings

2. I am technical user but would still like to take help of the SNS to make privacy settings

3. I am a non-technical user and would like SNS to automatically generate privacy settings for me

4. I am a non-technical user and would like to make my own privacy setting.

Based on the user's answer, SNS will then ask users to answer few more questions like I would like to share my pictures followed by the list of all the added contacts preselected by default. The users could de-select the ones with whom they do not want to share. Just like the implicit rule based approach, the framework also adopts the approach of graceful degradation which means it takes into consideration the fact that users can any stop answering the questions. However, the accuracy of the approach would be enhanced if the users answer all the questions at any time they wish. But, when the users stop responding to the questions then at that point the privacy preference model will take the input from the data or information visible to the users.

The modified user centered privacy framework suggests taking into account default and customized privacy settings for generating the final settings for the users in addition to the other two inputs. The proposed guidelines suggest that the default privacy policy should be stringent enough to protect users from unwanted privacy exposure.

The overall working of the user centric privacy model has been depicted through the flowchart in Figure 7. The flowchart shows that whenever the users joins the network then they are prompted with the question asking them for the permissions regarding privacy settings. Depending on the user's choice regarding making privacy settings the user centric privacy framework comes into action. If the users opts for option (a) and (d) then the framework performs no action whereas for options (b) and (c) it gets activated. After the framework has started it asks the users for their input in the form of answers to the asked questions. Once they stop feeding the input then its takes the input using the feature extraction functionality from their profile data. Apart

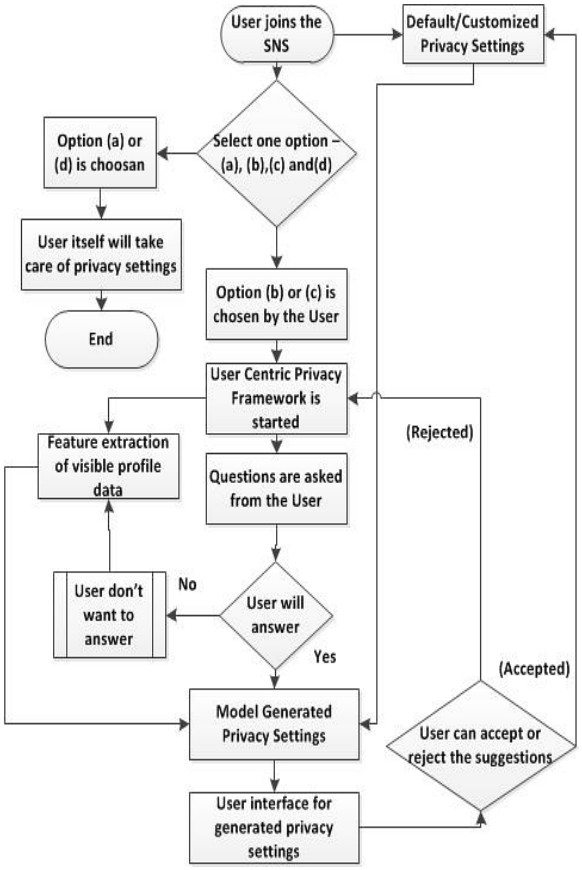

Figure 7: Flowchart showing the working of User Centric Privacy Model

from this it will also take input from the default privacy settings and customized privacy settings. The customized privacy settings can be termed as the privacy settings that has been done by the users themselves or the privacy settings that have been automatically generated by the User Centric Privacy Model at stage 5 as shown in the figure 6. We call the resulting settings of the User Centric Privacy Model as the customized because they are generated by taking user's input. After taking all the input, the framework generated some privacy settings depending on the current situation and prompts the user interface in the form of a dialog box (Figure 8) showing generated privacy settings to the users. They have the option of rejecting or accepting all the generates certain required privacy settings. Again, the further action is performed based on the user's input of accepting or rejecting the suggested settings. Regardless of what the user input is the user centric privacy model will start functioning again for generating the new privacy settings depending on the upcoming situations.

The framework takes the factor of scalability into its consideration as well. Whenever new contacts are added to existing contact list, privacy settings taking them into consideration will be generated. It will dynamically generates the settings after a span of few days. It will take into account the changed visible profile data and newly added contacts etc. It is difficult to quote the number of days after which privacy policies will be dynamically generated because the purposed model is not tested on a real set of data. It requires detailed

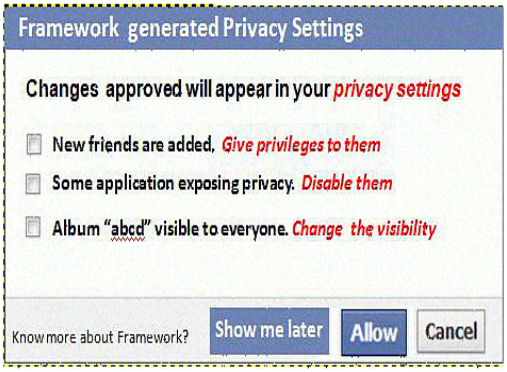

Figure 8: Dialog box for generated privacy settings

user studies and implementation of the prototype to compare different results. The system could also get feedback from the user whenever a new contact is added by asking the users some optional questions about giving access to their personal information while accepting or sending friend requests.

5 Discussion

Privacy is an important visible challenge in SNS. The social networking platforms are becoming popular as the user base is growing exponentially but privacy policies and settings are increasingly becoming difficult and complex to configure for an average user. Since privacy settings are the actual means for the users for controlling and managing their privacy in the on-line environment, so they should be always be designed and modeled keeping users in mind. The current situation as depicted in the paper through various examples of several popular SNS shows that present privacy policies and settings are failing in achieving the desired targets. As this poses serious threats to the privacy of the users hence, new approaches to modeling on-line privacy are being researched.

The paper discusses about the user-centric privacy model along with some design guidelines that could be used when modeling on-line privacy from user's point of view. The user-centric privacy model discussed in the paper has been inspired from the existing approach discussed in [7]. It takes into consideration the design guidelines for the modeling the user-centric privacy in the on-line environment. It is usable in the sense that it follows the concept of graceful degradation allowing the users to opt out at any time they want while providing input to the system. It is combination of different privacy settings i.e. default, customizable and adaptive. The user-centric privacy model also follows the guideline of increased awareness and visibility. Most of the time users are not aware what will happen if they make some changes. Hence, we purpose a dialog box to be prompted once the system generates some privacy settings for the users. The dialog box has been discussed later in detail. The users are also provided with the option of changing some of the settings if they want. If the users does not select all the options then

the system will again timely prompt the users with the new and unselected privacy settings until users cancel them. The framework also has an option for the users to make a choice if they never want to visualize the changed settings. If the user denies then the framework would automatically make the changes without bothering them again and again.

The user-centric privacy model can be further modified by taking into consideration reputation and recommendation factors. The framework has been proposed based on the explored literature. This is just a prototype and requires implementation and post testing to establish concrete results. User testing on some users can provide a brief view as how user reacts to this and what more needs to be done.

References

[1] E. Aimeur, S. Gambs, and A. Ho. Towards a privacy-enhanced social networking site. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pages 172 –179, 2010.

[2] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. A semantic web based framework for social network access control. In *Proceedings of the 14th ACM symposium on Access control models and technologies*, pages 177–186, New York, USA, 2009.

[3] L. Cutillo, R. Molva, and T. Strufe. Privacy preserving social networking through decentralization. pages 145–152, February 2009.

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

[5] G. Danezis. Inferring privacy policies for social networking services (position paper). In *AISec'09 : 2nd ACM workshop on security and artifical intelligence*, pages 5–10, 2009.

[6] A. Eldin and R. Wagenaar. Towards users driven privacy control. volume 5, pages 4673–4679 vol.5, October 2004.

[7] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *WWW '10: Proceedings of the 19th international conference on World wide web*, pages 351–360, New York, USA, April 2010.

[8] V. Garcia-Barrios. User-centric privacy framework: Integrating legal, technological and human aspects into user-adapting systems. volume 3, pages 176–181, August 2009.

[9] J. Hunker. A privacy expectations and security assurance offer system. In *NSPW '07: Proceedings of the 2007 Workshop on New Security Paradigms*, pages 15–22, New York, NY, USA, 2008.

[10] S. Kisilevich and F. Mansmann. Analysis of privacy in online social networks of runet. In *SIN '10: Proceedings of the 3rd international conference on Security of information and networks*, pages 46–55, New York,USA, October, 2010.

[11] M. McCandless. Managing your privacy in an on-line world. *IEEE Expert*, 12(1):76–77, January 1997.

[12] R. Saleh, D. Jutla, and P. Bodorik. Management of users' privacy preferences in context. pages 91–97, August 2007.

[13] E. Zheleva and L. Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World wide web*, pages 531–540, New York, USA, September, 2009.

[14] F. Zhu, S. Carpenter, A. Kulkarni, C. Chidambaram, and S. Pathak. Understanding and minimizing identity exposure in ubiquitous computing environments. pages 1–10, July, 2009.