Privacy Settings on Facebook: Their Roles and Importance

Siti Zainab Ibrahim, Ann Blandford, Nadia Bianchi-Berthouze

UCL Interaction Centre
University College London
WC1E 6BT, United Kingdom
siti.ibrahim, a.blandford, n.berthouze@ucl.ac.uk

This explorative study aims to gain insight about which privacy settings and features on the interfaces are commonly used by Facebook users. User data was collected using an online survey. Based on the survey data, a set of the commonly used privacy strategies on Facebook were identified. We found that these strategies were mainly used to manage three types of privacy concerns: 1) personal profile visibility, 2) personal networking boundary, and 3) personal privacy awareness. A point-biserial correlation analysis revealed that only networking privacy strategies were significantly correlated with the feeling of control users felt in mitigating hackers, blackmailers, stalkers as well as compromising relations and job positions. Hence, when the goal of the sites is to empower users for protecting their privacy, it is important to understand how users make decisions with the help of these privacy settings and features on user interfaces. Implications of these findings as well as suggestions for future research are discussed.

Social network sites; privacy settings; sense of control; privacy design

I. INTRODUCTION

A survey study in 2006 by Acquisti and Gross found that users do not understand how privacy settings on Facebook work [1]. However, user attitudes towards privacy in social network sites appear to have changed significantly over the next four years. Another survey study by boyd and Hargaitti [6] in 2010 found that 98% of their respondents had previously modified at least one of the privacy settings on the site. Users were found to frequently change their privacy settings on Facebook “in response to media reports of Facebook changing the defaults” [8].

The increase in awareness about the changes constantly made by Facebook, the increase in numbers of privacy breaches and the need to protect privacy have somehow elevated the significance of privacy settings on Facebook. However, there are loopholes in the design of the existing privacy settings. Despite using the settings, users are still exposed to privacy risks and vulnerable situations. For instance, Egelman et. al [8] found that the existing visibility access settings on Facebook do not keep personal information inaccessible by unintended audience. Another study by Aimeur and colleagues [2] found that 26% of respondents of their survey admitted that they have already disclosed to other people some photos and comments of their friends without consent. From these studies, we come to a conclusion that privacy risks and vulnerable situations may not be addressed effectively even by modifying privacy settings on Facebook alone.

These design loopholes may potentially occur when developers do not realize the social norms of which the sites are used and the implications to privacy when people make their personal information easily accessible by others. In response to these problems, various design solutions have been proposed [2,4,8,16,20]. However, we have yet to witness the extent to which these solutions have impacted the design of user interfaces and privacy settings of many social network sites. The slow adoption by the sites suggests two possible reasons for this situation: (1) the solutions do not share similar business interests of the sites where the survival of these sites depend on how they leverage user data, and (2) the design of these solutions are not user-driven; therefore lacking evidence to show to those sites that they are what users opt for.

Due to various privacy settings and features that are available on Facebook, it is not known how they are used strategically among users. Thus, this study aims to investigate what are the commonly used privacy strategies among Facebook users. This investigation would potentially help in revealing privacy settings and features that are effectively useful for users to manage their privacy on the site. We also complement our analysis by looking at the least used privacy strategies on Facebook. In relations to features and privacy settings on the user interfaces of Facebook, we also investigated the implications of using the privacy strategies on the sense of control felt by users in mitigating or minimizing potential privacy risks.

The outline of the paper is as follows. We first present the privacy model of Facebook by highlighting the design of its privacy settings. Next, we introduce the privacy issues that result from poor design of privacy settings on Facebook. Some existing solutions to these issues are also briefly discussed. Section IV outlines the design of our online survey, follow by the analysis of the results. Finally, we conclude by discussing our results and pointing to future research.

II. FACEBOOK’S PRIVACY MODEL

In comparison to other major competitors, Facebook is chosen because it is the most popular social network site in the world. Facebook is available in more than 70 languages. According to Facebook statistics [11], by December 2011, Facebook had 845 million monthly active users, with 483
million daily active users. Its mobile users account for 425 million monthly active users. Facebook is regarded as an international player with regards to privacy and security. It receives wide media coverage about privacy and security issues. In response to those issues, Facebook has been actively involved in addressing various privacy issues such as by making its privacy features simpler and easy to use [25], and by committing to make Facebook a safer environment for sharing and socializing [12].

In its lifetime, Facebook has performed several major changes to its privacy settings. Users’ feedback, regulation requirements and business needs are some of the major reasons that drive the changes. In May 2010, Facebook reduced the number of its privacy settings. Previously, there were 50 pieces of information that required tweaking in order to make them private, and a total of 13 privacy pages. The new changes reduce the number of privacy tweaking to 15, and privacy pages to 8.

Overall, Facebook has extensive privacy settings, controlling access to nearly all personal information. The settings are accessed through a privacy link displayed on the top right of a user’s profile. This link brings up a privacy settings page with six privacy categories (refer Figure 1). Each of these links, some of which link to additional sub-pages, opens a page of menus and checkboxes to set privacy levels or to control information flow.

Facebook currently permits privacy settings to be configured for basic information and for each data type. Basic information has a separate setting for each field; these fields include gender, religions, views, interests, and activities. These fields tend to be fairly static; users rarely update their gender, religious views, etc. For data types (e.g. photos, notes, links, events, and status updates), which tend to be more dynamic, the user is able to select default settings per type (see Figure 2). This granular design further reduced the number of privacy settings and privacy pages.

A survey study by Liu and colleagues reveals that while users are uploading significant amounts of content to Facebook, almost half of the content is shared with the default privacy settings, which expose the content to all Facebook users [17]. Users in their survey reported that this was the desired setting only 20% of the time, suggesting that the default settings are poorly chosen. More worryingly, even for photos for which the privacy settings have been modified by the user, the modified privacy settings match
users’ expectations less than 40% of the time. This strongly suggests that users are having trouble correctly configuring their privacy settings. Liu and colleagues examined the potential for assisting users in managing their privacy. Specifically, they focused on friend lists, a mechanism for users to group their friends that is similar to the Circles feature of Google+. They explored whether the friend lists could be automatically populated using community detection algorithms over the social network.

Gurses, Rizk and Gunther have introduced their analytical framework for privacy breaches in social network sites [14]. They selected from greater pool of privacy breaches in social network sites mentioned in news and blogosphere. Four categorizations of privacy breaches were presented:

1) Indeterminate visibility: a user’s profile information being visible to others without the user’s explicit knowledge or approval.

2) Separation of Digital Identities and Aggregation: a user’s inability to create multiple profiles on a given social network site or in different digital environments.

3) Contested Ownership: complications in ownership with respect to relational information and aggregated data between users, as well as with the service provider.

4) Misappropriation: the use of data in social network sites that is out-of-context or for previously undefined purposes.

From identification of these breaches, they list possibilities of intervention and negotiation heuristics for user-driven interface design in social network sites.

Lipford et. al. [16] created AudienceView, a prototype privacy settings interface for social network sites. Rather than modifying settings with a set of menus and checkboxes, users view pages of their profiles from the point of view of different audiences, e.g. different groups of friends, networks, public, etc. This interface provides a more visual and accurate mental model of what different people can view of them, allowing users to more explicitly and concretely consider the context of their information and adjust that information flow as desired. AudienceView was inspired by the authors’ exploration on privacy issues on social network sites through the lens of contextual integrity [19]. Their exploration implies that one way to improve privacy management, and help users achieve their desired privacy levels, is to make the norms of appropriateness and distribution of information flow more visible.

User Privacy Policy (UPP) was proposed by Aimeur, Gamburg, and Ho to provide users with an easy and flexible way to inform and enforce (in the form of contract) their privacy concerns to other users, third parties and SNS service providers [2]. This UPP is based on privacy framework that was informed by the results of their survey. From their survey, they discovered that half of the participants (51%) would be willing to spend time on processes designed to protect their privacy, but only 38% always check all the privacy settings available, although 45% of the users state that they look at the privacy settings link to information that they consider as important. Moreover, it is not always clear to the user how to block unwanted person from messaging him or prevent him from accessing his personal information (34%). They also feel that their social network provider do not warn them enough about the risk of divulging some of their information online (76%).

Another study by Egelman, Oates and Krishnamurthi found that without relevant feedback, participants would have introduced errors into their privacy policies a majority of the time [8]. Their errors were more likely to result in sharing with unintended parties (data leakage) rather than denying access to authorized users. Their data show that when ambiguities were detected and relevant guidance was offered, users took the time to edit their privacy settings. As a result, they designed a new interface for specifying access control settings on Facebook using a visual metaphor: Venn Diagrams. They reasoned that the act of specifying an access control policy on Facebook is a matter of indicating how the intersections of a user’s networks should be granted access.

To the best of our knowledge, none of the previous solutions so far solves all the privacy risks, and it’s partly because they are all built from the researchers’ perspectives rather than users’ perspectives. Although those studies managed to identify privacy issues with privacy settings on Facebook, the design and implementation of those solutions are not driven by the users themselves. In the area where privacy problems cannot be addressed by the existing privacy settings, few past works have indicated that users are indeed very creative in adopting the non-privacy features on the user interfaces to protect their privacy [5,21].

IV. Methodology

Our study investigated the most used privacy strategies on Facebook, and how they help to promote positive experience and secure feeling among users. We conducted an online survey from October 18, 2011 until November 17, 2011. We limited the participations for the survey only to Facebook users. The online survey was hosted on the commercial Smart Survey system. It was piloted prior to large-scale distribution to Facebook users. A copy of the survey can be obtained by sending an email to the first author. To encourage participation, the link to this survey was also shared on several Facebook community pages. The respondents were also approached via various technological means such as departmental mailing lists and electronic research subject pool system. All respondents were entitled to enter a draw, with chances of winning a £25 Amazon voucher.

A. Online Survey
The survey consists of two important sections: (1) privacy strategies, and (2) sense of control.
1) Privacy Strategies – A Multiple Response Set: The first section lists a group of privacy strategies users can perform on Facebook in safeguarding their privacy. For the purpose of this study, we only included privacy strategies that used features and privacy settings on Facebook’s user interfaces prior to October 18, 2011. Not included in the list are privacy settings related to location-based, application platform and mobile networks. These three privacy settings were excluded from the survey because they involved ‘intangible’ information of which the privacy management for such information is dealt with directly between Facebook and service providers. With this intangibility, users have no direct control over the security and protection of such information, making this risk difficult to explain and understand.

Based on these sources [24,21,5,10], we developed 38 Facebook privacy strategies. All items were measured as a dichotomous value of either ‘Yes’ or ‘No’; each means ‘I use the strategy’ or ‘I do not use the strategy’ respectively. We asked respondents to select strategies that were applicable to them. In order to encourage respondents reading through all the 38 items, we divided these items into five categories. The division was made in the hope that it would be able to retain respondents’ attention throughout the session. The items were divided based on main privacy functions discussed in Facebook’s Data Use Policy and Help Centre pages [9,10]. There are five important divisions of privacy strategies:

a) Security: All privacy strategies that are used to protect respondents’ Facebook accounts from potential intruders.

b) Tagging: The use of features and privacy settings that allow respondents to monitor activities on how other users link them to something they post. At the same time, tagging also allows respondents to control the visibility of any posts they were tagged in.

c) Sharing: All the use of features and privacy settings that help controlling the visibility and accessibility of items respondents posted to others.

d) Searching: Allow other people to search for respondents’ profiles via Facebook’s search utility or general public search engines.

e) Filtering: Interface features and privacy settings that are useful to select preferred posts and updates from other users as well as to accept new friend requests.

2) Sense of Control: This variable measures the sense of control users felt in mitigating or minimizing occurrences of a set of potential privacy risks on Facebook. We collated 11 privacy risk items from two previous survey studies: [22] and [23]. In the survey by Rosa and colleagues [22], using a pool of privacy threats, respondents were asked to select privacy risks that they were most concerned with when using social networks. Meanwhile, Stutzman, Capra, and Thompson [23] constructed a variable consists of a list of potential risks that may affect personal information respondents disclosed on Facebook.

Based on these sources, the selected privacy items for this survey pertain to users’ concerns about data security and potential intruders to their Facebook accounts. The items also include deliberate misuse of information that may affect position at work, personal relationship and embarrassment to self. The response categories for each item were ranging from ‘No control at all’ to ‘Completely in control’, represented on a 5-point Likert-scale. Reliability analysis was used to make sure that the items are consistently reflecting the sense of control construct that this variable is measuring [13]. Overall, all items for sense of control variable contributed to an excellent reliability with Cronbach’s α = .935.

B. Participants

139 respondents completed the survey. Respondents ranged between 18 and 54 years of age (Mean = 31.42, SD = 0.689). Almost half of the respondents (46.76%) were aged between 26 and 34. Out of 139, 92 respondents are female. In terms of Facebook demographics, more than half of the respondents (64.2%) have used Facebook for more than 3 years.

V. ANALYSIS OF THE RESULTS

In this section, we present results from our survey, and discuss the regression analysis between the most used privacy strategies and the sense of control.

A. The Most Commonly Used Privacy Strategies

We use multiple response analysis to identify the most commonly used privacy strategies used on Facebook. The dichotomous set was constructed by calculating value ‘1’ for all privacy strategy items. This value indicates that participants used the strategy on their Facebook accounts. Out of 38 privacy strategy items, we only consider privacy strategy items that have more than 50% of cases (i.e. more than half of the respondents reported to have used the strategies). From these strategies, we identified three important purposes that classify the used of these strategies.

1) Managing Personal Profile Visibility: Table I below shows the most used privacy strategies to limit access for certain audience to a set of personal information shared on Facebook. The need to manage the visibility of the profile by imposing some boundaries to personal information is probably driven by the norm of “appropriateness” and the norm of “distribution” of information flow; two concepts devised by Nissembera [19].

In relation to “appropriation” norm, this study found that users excluded certain information, limiting access to their profile pages and posted contents, restricting sharing to certain audiences, and sending private messages instead of posting on public spaces. As for the “distribution” norm, users demonstrated the norm when Facebook applications published on users’ Wall about their activities when they...
used that application. In order to gain control over the application, users chose to block posting from applications on their News Feed.

In addition to these norms, our finding suggests that users also need to manage visibility in terms of: 1) increasing visibility as an individual beyond user’s existing network, 2) ensuring that the personality user portrays on Facebook Wall and profile page look accordingly to a specific audience, including non-Facebook users in the public, and 3) controlling privacy breach by other people over user’s expectations of what is appropriate and acceptable. For example, although “tagging” is an efficient and convenient method of sharing a photo with the people in it although this goes against offline social norms [16], this feature reduces the control that people have over the sharing and distribution of their own pictures.

2) Managing Personal Networking Boundary: Who become one’s friends on Facebook is also one privacy concern of many Facebook users. According to our survey, the strategies in Table II below were commonly employed for managing user’s personal networking boundary. These two strategies complement each other in the sense that in order to get to know the person who has issued a friend request, user will scan their profile for information.

TABLE II. STRATEGIES FOR MANAGING NETWORK BOUNDARY

<table>
<thead>
<tr>
<th>Privacy Strategies</th>
<th>Yes Responses (Count)</th>
<th>% of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>I only accept new friends if I know them in-person offline.</td>
<td>104</td>
<td>75.4%</td>
</tr>
<tr>
<td>Prior to accepting new friend requests, I scan their personal profile.</td>
<td>94</td>
<td>68.1%</td>
</tr>
</tbody>
</table>

3) Managing Personal Privacy Awareness: Table III below lists the most used privacy strategies to manage privacy awareness. The results show that users did keep track on what is happening on Facebook and how the changes made by Facebook may impact their privacy. This is supported by another study [2] that shows that 76% of their respondents felt that social network sites’ providers do not warn them enough about the risk of divulging some of their information online.

TABLE III. STRATEGIES FOR MANAGING PRIVACY AWARENESS

<table>
<thead>
<tr>
<th>Privacy Strategies</th>
<th>Yes Responses (Count)</th>
<th>% of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>I customized which applications and features can send notifications to my email</td>
<td>88</td>
<td>63.8%</td>
</tr>
<tr>
<td>I change my default privacy settings every now and then</td>
<td>72</td>
<td>52.25%</td>
</tr>
</tbody>
</table>

B. Do Commonly Used Privacy Strategies Make Respondents To Feel More in Control of Their Privacy?

Our point-biserial correlation analysis between the most used privacy strategies and the sense of control felt reveals that only privacy networking boundary strategies are significantly correlated with the control feeling users experience in mitigating or minimizing certain privacy risks. Due to limited space, Table VI shows only significant correlations from the analysis.

There is a negative correlation between adding friends known offline and the control to reduce the potential of being stalked by someone (r = -.188, p < 0.05). This may suggest that by adding people who users know offline reduce the worry from being stalked by strangers. We also found that users gained more control to prevent hackers and blackmailers as well as reducing potential for compromising relations and job positions by scanning profile pages of those people who requested to become their friends on Facebook.

We also extended our analysis by looking at the patterns of privacy strategies used between users who felt less in control and users who felt more in control of their privacy on Facebook. The mean score for each respondent is calculated by dividing the total score of all items in the ‘sense of control’ variable by the number of items. Then, the mean value for all the mean scores were calculated (Mean = 2.87, STD = 0.92). Respondents who have mean score less than the mean value are classified as ‘less in control’, while ‘more in control’ is for those with mean scores higher than the mean value. 45% (N = 63) of our respondents are ‘less in control’, and the rest belongs to ‘more in control’.

For each user group, we performed multiple regressions (stepwise) between independent variable: all commonly used strategies (entered according to the percentage of cases, from the highest to lowest), and dependent variable: control level. We found no significant correlations for the ‘more in control’ group.
As shown in Table V, we found significant relations between the use of three Facebook privacy strategies and perceived sense of control for users who felt less in control over their privacy on Facebook. Users who felt less in control were found to use less private messaging, have tendency not to share personal information on the site, and permit other Facebook users to search for their profile. We can say that these three privacy strategies shares 23.7% ($R^2$ in percentage) of the variability in the sense of control among users who felt more vulnerable to privacy risks. This leaves 76.3% of the variability to be accounted by other factors such as demographic and personality attributes.

Regardless of the lower control users felt about their privacy on Facebook, the tendency to connect with others does not limit them from letting their profile to be searchable by other users. By exposing their profiles to all Facebook users, the vulnerability that they felt may lead them to exclude their personal information on the site. This finding is consistent with findings from [16] where they found that users do expect their profiles to be viewed by a large and public audience. These users are attempting to tailor their profile information with the risks associated to that expectation.

The less use of private messaging also may contribute to the increase in vulnerable feeling (due to less control) experience among these users. This may suggest that this group of users prefer more open spaces on Facebook such as timeline for communicating with friends. Given the amount of personal information that was posted in these open space, the degree of vulnerability increases causing users to feel less in control regardless of the strategies they used.

### TABLE V. Regression Summary Between Privacy Strategies and 'Less in Control' Respondent

<table>
<thead>
<tr>
<th>Dependent Variable:</th>
<th>Less in Control (Mean scores)</th>
<th>SSE</th>
<th>4.148</th>
<th>F-Test</th>
<th>6.108</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standard Estimate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Standard Error</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>t-stat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prob &gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[t]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Constant)</td>
<td>2.102</td>
<td>0.155</td>
<td>13.537</td>
<td>0.000</td>
<td></td>
</tr>
<tr>
<td>Profile Search</td>
<td>0.335</td>
<td>0.122</td>
<td>2.897</td>
<td>0.005</td>
<td></td>
</tr>
<tr>
<td>Private Messaging</td>
<td>-0.361</td>
<td>0.160</td>
<td>-3.023</td>
<td>0.004</td>
<td></td>
</tr>
<tr>
<td>Exclude Information</td>
<td>0.537</td>
<td>0.131</td>
<td>2.797</td>
<td>0.007</td>
<td></td>
</tr>
</tbody>
</table>

Note: MSE = sum of squared errors; DFE = degrees of freedom associated with the error term; MSR = mean square error; DF = degrees of freedom; t-stat = t-statistic; Prob = probability

C. Additional Insights: The Least Used Privacy Strategies

To complement our analysis of the commonly used privacy strategies, we include an overview of the least used privacy strategies on Facebook as listed below.

- I deactivate my Facebook accounts every now and then (25%).
- I enabled login notifications (24.5%).
- I limited certain friends from having access to old posts on my Wall (22.3%).
- I give permission for people on the Internet to search my Facebook profile using public search engines (e.g. Google) (18%).
- I provided fake or inaccurate information to restrict people I don’t know from gaining information about me (14.4%).
- I added a person or application that I have hidden back to my News Feed (10.1%).
- I generated specific passwords for applications (5.8%).

The least used privacy strategies are those that were used by less than 25% of the participants, as indicated in the bracket. We could observe that three of the least used privacy strategies involve security aspects of the site: (1) account deactivation, (2) login notification, and (3) access password. Having only few participants faking their own information (14.4%) on the site suggests that many users reveal their true identity and real information on the site. Meanwhile, 10% of the participants reported that they unblocked strategy for stories suggesting that blocking may be an effective way to manage certain privacy conflicts.

VI. DISCUSSION & CONCLUSION

This paper investigates the privacy strategies that are commonly used by users, and to determine whether they help users feel in control of their privacy on Facebook. The study found three categories of privacy strategies that are commonly used by Facebook users: (1) managing profile visibility, (2) managing networking boundary, and (3) managing privacy awareness. This finding suggests that social network sites in general, and Facebook in particular, should give more attention to designing and implementing privacy settings and features that can further support those strategies.

Our finding also shows that the privacy strategies may either involve direct use or indirect use of the interfaces for managing privacy on the sites. Our analysis reveals that profile visibility strategies and privacy awareness strategies all involved the use of existing interface features and privacy settings on Facebook. Meanwhile, networking boundary strategies indirectly utilized certain social-oriented features on the interfaces. For example, there are no recommendation utilities on the interface to assist users as to
whether to reject or accept a new friend request. To help making their decisions, users may scan for mutual friends and profile pages to gather necessary information before acting on the request. This evidence suggests that certain social-oriented features on Facebook also serve privacy purposes for some users.

Although we used 50% of cases as an indicator for a privacy strategy to be categorized as a commonly used strategy on Facebook, the other half of the percentage does not suggest that users decided not to use them. For example, in Table I, we found that nearly 53% of our participants customized the audience for particular content, 51% allow other Facebook users to search their profile, and 50% review tags made by their friends. Nearly half of the users did not use those three strategies. The existence of a single default setting may suggest why some users did not customize privacy settings for a single new post they made on Facebook. Some users may not be aware that by default other Facebook users can search for their profile, and that Facebook provides tool such as tag review.

On the other hand, those least used privacy strategies among Facebook users may suggest that certain privacy settings and features on the site require improvement or reconsideration. The low utilization of those settings and features may suggest either Facebook users do not know of their existence, users simply find them less useful due to other attractive alternative strategies, they do not provide what users expect for effective privacy management on the site, or users have no need to use them at all.

This paper also provides insight into Facebook privacy settings and users’ understanding and usage of these settings. It looks at the correlation between the feeling in control users felt and the most commonly used privacy settings on Facebook. We hope that this study may shed some light on users’ thoughts in terms of the importance of certain privacy settings and features to effectively manage their privacy on the site.

Since convenience sampling [3] was used to sample our respondents, the generalization of the results to Facebook population must be made with care. A part of the reason is because our sample does not represent the overall distribution of Facebook population based on age since we did not include teenagers in our survey who constitute 20.6% of Facebook users [11]. For the study to be significant and representative, future studies should devise a sampling approach that could capture all possible demographic profiles of Facebook population.

In addition to the limited generalization of our finding, we also did not extend our investigation on the demographics effects to our results. We would recommend future investigations to specifically looking at how various demographic profiles affect: (1) the most commonly use privacy strategies and (2) their relations to the feeling in control are affected by various demographic profiles.

There are also several limitations to using an online survey to study human attitudes and behaviors towards privacy. Using the survey method can present the problem of conveying insufficient and biased information. This is further supported by boyd and Marwick [5] who claimed that privacy must be contextualized because users’ understanding of privacy and how they use privacy settings vary by individual, by community, by situation, by role, and by interaction.

Moreover, previous surveys also show that privacy attitudes that are collected using surveys may not always be consistent with actual privacy behaviors [15]. As people move through different levels of privacy experience during social interaction on the sites, assessing it is complex and requires understanding of users’ psychology and behaviors. Users also often demonstrate an observable different behavior before and after unexpected changes to privacy in the sites. In this situation, users often describe how they tactically changed their behavior to interact with the unexpectedness. In the future, this behavior change should be observed in real-time using proper techniques for user study, combined with user’s retrospective reports or with post-experience interviews.

Another limitation is that there is also a potential where we do not include all possible privacy strategies on Facebook. Our items for this variable are collated from literature published before August 2011. As Facebook keeps on changing its interfaces and privacy settings, certain privacy strategies may become invalid today. Therefore, certain survey items for privacy strategies may eventually be adapted, modified or removed from the survey in future studies.

Following this study, our next step will be to investigate how the existing design and implementation of privacy settings and social features influence users’ understanding about privacy on Facebook. Guided by these commonly used privacy strategies, we will select a set of privacy settings and social features that are commonly used by users for strategizing their approach towards privacy on Facebook. The finding from this study may be useful for us to help defining the scope for a user study using Facebook. Given the complexity of privacy settings and social features on Facebook, knowing which settings and features are commonly used by the users (or less useful) helps to reduce the ambiguity of selecting specific aspects of the site for further investigation.

REFERENCES


