VOL. 10, NO. 23, DECEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PERCEIVED BENEFITS, PRIVACY RISKS AND THE USED OF PRIVACY STRATEGIES ON FACEBOOK: AN EXPLORATIVE STUDY

Siti Zainab Ibrahim[1] and Maslin Masrom[2]
[1] Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia
[2]UTM Razak School of Engineering and Advanced Technology, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
E-Mail: sitizainab.ibrahim@mmu.edu.my

ABSTRACT

This explorative study aims to gain insight about which privacy settings and features on Facebook interfaces are commonly used by Facebook users, and how perceived benefits and privacy risks for personal information disclosure on Facebook influences privacy strategies used on the site. Online survey was used to gather user data. Analysis of the survey data revealed the privacy strategies on Facebook were most commonly used for managing profile visibility, networking boundaries, and privacy awareness. Using a point-biserial correlation analysis, the results demonstrated significant relations between the types of privacy strategies used on Facebook and the types of perceived benefits experienced from using Facebook. Significant relations were also observed between the types of privacy strategies and the types of concerns for privacy risks on Facebook. Hence, when the goal of Facebook is to empower users for protecting their privacy, it is important to understand how users make disclosure decisions with the help of these privacy settings and features on user interfaces. This paper concludes with remarks on the importance of understanding users' attitudes in educating them about privacy protection in social applications.

Keywords: perceived benefits, privacy risks, privacy strategies, social network sites.

INTRODUCTION

Facebook is the most popular social network site in the globe [1]. As of June 2015, there were 968 million daily active users on Facebook, with approximately 83.1% of these users were outside of the US and Canada [2]. Facebook is well-known across the globe with regards to security and privacy issues. For example, Facebook has been reported sharing user data with advertisers and third-parties [3], constantly changing privacy features [4], obnoxious default settings [5] and privacy policies [6], and the recent case was about outsourcing practices [7].

Bonneau, Anderson and Church [8] argue that Facebook was having a large number of privacy settings in comparison to its competitors. These intensive privacy settings acquire a strong commitment from its users to learn and understand the implications of using them to their privacy. Users needed to spend a large amount of their time and spent their effort to configure each privacy setting. This sort of demands was further amplified when Facebook rapidly evolved by constantly introducing new privacy regulations via the implementation of its privacy settings. The constant evolution has promoted a poor mental model among its users about how privacy settings work on Facebook [9].

Strater and Lipford [10] also revealed that there were several issues with privacy settings on Facebook. There were inconsistencies in the implementation of certain privacy settings. For example, Facebook's privacy policy in 2012 mentioned that users' profile pictures were viewable to the public audience by default. However, the implementation of inline privacy setting for profile picture which allows users to select a specific audience for the photo gave an impression that it was only viewable to the selected audience, not to the public audience. Participants in this study also had reported on having poor knowledge about how privacy settings on Facebook worked. They were also confused by the actual implications from using those settings to their privacy. Some participants were not aware about the existence of certain privacy settings on Facebook, such as 'untag'. Users also found that it was challenging to adjust and remember the most basic privacy settings. Limited visual feedback and confusing languages might have contributed to these difficulties users have been experiencing with privacy settings on Facebook [9].

Due to the challenges presented in previous literature, this study aims to investigate the most common privacy strategies used on Facebook. In addition, the relations between the used of common privacy strategies on Facebook and these two users' perceptions: 1) the perceived benefits of using Facebook, and 2) the concerns for privacy risks were further explored. This exploration is necessary because the used of privacy strategies are mainly driven by concerns over certain privacy risks and vulnerable situations on Facebook [11][12]. However, the perceived benefits gained from using Facebook have compensated these concerns, thus, influenced the strategic efforts used in protecting privacy [13].

We begin this paper by giving an overview on Communication Privacy Management (CPM) theory and how benefit-risk assessments inform privacy decisions. A brief overview is presented on privacy settings offered by Facebook. Later, a detail account of the design and construction of our online survey is described. In further sections, the results and discussion of multiple responses analysis and correlation analysis that were applied on the collected data are presented. The multiple responses analysis helped us to identify the most commonly used privacy strategies on Facebook. By extending the finding, we presented the results of several point-biserial correlation analyses in investigating the relations between the most commonly used privacy strategies, the perceived benefits of disclosure on Facebook, and the concerns on privacy risks.

THEORETICAL FRAMEWORK

Communication Privacy Management (CPM) is a theory that illustrates a rule-based system. The theory describes the way people make decisions about achieving balance between being public and private [14]. In comparison to other privacy theories [15][16], CPM emphasizes on communication as the core that underlie the process of disclosing private information to the public. This emphasis greatly reflects Facebook which has become one of the technological means where people could easily and openly share their personal information and stories about themselves with other people of whom they are connected with on the site.

Some information of oneself is deemed private because revelation of this information to others may expose that person to certain degrees of vulnerability. CPM uses boundary metaphor to mark the ownership lines of such information. One of the criteria used to regulate this privacy boundary is the assessment of benefits and risks due to information disclosure. This criterion explains why despite of many privacy concerns associated with revealing personal information on Facebook, people keeps on sharing huge amount of information on this site because of the social benefits they gained from sharing [13][17][18].

There are many benefits gained from disclosure of personal information on Facebook. Previous studies found that besides entertainment [19]–[21], Facebook was mainly used as a medium to express oneself [22][23] as well as to maintain new and existing relationships [13][24]. Overtime, the privacy settings provided by Facebook has created an environment in which allowing users to perceive that their personal space on Facebook is indeed safe and private [11]. This perception has, overtime, encouraged users to increase the amount and scope of personal information they disclosed on the site [25]. Although few studies revealed that users did not hold high confidence on the use of privacy settings due to information leakage and mismatch of disclosure expectations [10][26][27], alternative privacy strategies were devised in order to protect their personal information in order to reap as much benefits from sharing on Facebook [28][29].

Besides motivated for gaining the benefits of using Facebook, the increase usage of privacy settings was also driven by the elevated concerns on privacy risks on the site. Many studies have found significant positive correlations between the used of privacy strategies and concerns on privacy risks on Facebook [30]–[32] . The study by Strater and Lipford [10] has revealed that the participants' expectation of outcomes of their privacy settings did not match the actual outcomes. The mismatches between expectations and the actual outcomes resulted in accidental disclosure where personal information was also viewable to unintended audience which would be very difficult for users to detect. Eventually, some users were reported to learn these mismatches through their own experiences and the social norms among their peers. Even after modifying those settings, users could still experience difficulty in ensuring their settings match their expectation [9]. Users also have reported that that it was difficult to experiment with the privacy settings on Facebook. There is lacking of interface utilities and visual feedbacks that could inform users about the outcome of using various privacy settings [10]. Due to these limitations, teens in the US devised their own privacy strategies to protect their privacy. For example, they used blocking features to limit visibility and actions to others [29], and de-activated their accounts to create visibility cloak for Facebook usage [33]. Even some users prefer to remain anonymous in social networks [34].

Our observations from previous studies between benefit-risk assessments and the use of privacy strategies have lead us to seek answers for the following two questions:

RQ1: What are the most common privacy strategies used by Facebook users?

RQ2: Does significant relations exist between perceived benefits and the use of certain privacy strategies on Facebook?

RQ3: Does significant relations exist between concerns on privacy risks on Facebook and the use of certain privacy strategies?

PRIVACY SETTINGS ON FACEBOOK

In its lifetime, Facebook has performed several major changes to its privacy settings. Users' feedbacks, 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 fifty pieces of information that required re-configurations in order to make them private, and a total of thirteen privacy pages. The new changes had reduced the number of privacy re-configurations to fifteen, and privacy pages to eight [5].

Overall, Facebook has intensive privacy settings that provide access control to almost all personal information. Currently, Facebook implements privacy settings on basic personal information, and audience customization can be made for each data type. Each field in basic information has a separate setting; these fields include gender, religions, views, interests, and activities. These fields tend to be static where users rarely update their gender and religious views. For data types such as photos, notes, links, events, and status update which tend to be more dynamic; users are able to select the default audience for each new post made on Facebook.

METHODOLOGY

Following an examination of several survey-related works which investigated privacy in various social network sites, a set of privacy items was collated. The collated items were drawn from various sources [35]. The items are divided into three main measures: 1) the perceived benefits of sharing on Facebook, 2) concerns on privacy risks on Facebook, and 3) privacy strategies available on Facebook. The development of these measures is each described in more detail in the following sections.

Perceived Benefits

Table-1. Perceived Benefit Items.

Perceived Benefit Items
- To express my feelings to others.
- To increase my popularity
- To publicize events and news
- To promote and sell expertise/products
- To reveal my private thoughts about certain issues.
- To reinforce my values and views.
- To show information about myself
- To meet new people
- To keep in touch with people
- To learn about other people
- To find contact information
- To influence other people view about an issue.

These twelve items measures the benefits as perceived by respondents gained from using Facebook. In these measures, we asked respondents to indicate the level of usefulness of Facebook in terms of allowing them to achieve their goals or satisfying their social needs. Respondents were asked to indicate "how useful is Facebook to [you] to do the following?' The response categories were 'not useful at all' to 'highly useful' represented on a 5-Likert scale. Our perceived benefit items are summarized in Table-1 above.

'To express my feelings to others', 'to reveal my private thoughts about certain issues', 'to reinforce my values and views' and 'to influence other people view about an issue' items were derived from CPM theory [14]. Based on survey items on why people used social network sites from [34] and the reasons that motivated people to socialize in social networks [11], we included the following benefit items into our list: 'find contact', 'publicize events and news', 'meet new people', 'keep in-touch with people', 'promote and sell expertise/products', 'learn about on-going updates of other people', 'show info about myself' and 'increase popularity'. The perceived benefits items all have high reliability with Cronbach's α = .881 (greater than .70 based on [36]).

Concerns for Privacy Risks

Respondents were asked to indicate the degree of concerns with regards to the potential privacy risks that might arise upon disclosing their personal information on Facebook. A set of privacy risk items was created by combining survey items from previous literature. The privacy risk items chose from [34][30][37] represent a set of data-related privacy risks that were mainly concerns about the security and protection of users' data from potential intruders. Many users in social network sites are concerned about deliberate misuse of their personal information, as well as on privacy lost that relate to possible criminal activities and those that might lead to security problems [34]. The selected items are 'hackers', 'identity theft', 'cyber stalking', 'information leakage' and 'blackmail'.

Because of the dynamics in social interactions that occur on Facebook, we also acknowledged that users were also exposed to privacy risks that are social in nature. For example, the information shared on Facebook may be used to perform gossip, thus, causing social conflicts among wider audience [38]. As such, based on the risks of disclosure discussed by CPM theory [14], six new social privacy risk items were added. The items are 'discredited', 'broken relations', 'compromised relations', jeopardizing job position', 'motive misinterpretation', and 'casted aside by family/friends/society'. The response categories for each risk item were 'not concern at all' to 'very concern', represented on 5-Likert scales. Table-2 below summarizes the concern items for privacy risks on Facebook. The reliability of these scales is high with Cronbach's α = .934 (greater than .70 based on [36]).

Table-2. Concern Items for Privacy Risks.

Concerns for Privacy Risk Items
- Hackers
- Identity theft
- Cyber stalking
- Discredited
- Casted aside
- Misinterpreted
- Blackmail
- Information leakage
- Compromised relations
- Broken relations
- Jeopardizing job position

The Types of Privacy Strategies

We collected a set of privacy strategies from three major sources: 1) Facebook Help Centre [39], 2) [38], [40] and 3) [41]. We did not limit the strategies to privacy features on Facebook. The reason was because we found that certain users achieved privacy by using various means that were beyond the privacy features offered by Facebook. Previous studies such as [38][33][41][42] found that there were certain non-privacy Facebook features which were appropriated by users to manage their privacy (e.g. deleting post feature). There were also few occasions where users did not use any Facebook privacy features to manage their privacy (e.g. self-coded messages). Due to an exhaustive list of privacy strategies, we divided the strategies based on the protective functionalities they provide.

Table-3 below shows the privacy strategies grouped under five categories. The first group is security strategies which refer to all strategies used to protect one's Facebook account from potential intruders. For the second group, we used the tagging definition by Facebook [39]. Tagging strategies means one could monitor how other users in Facebook link oneself to something they post, and at the same time, providing oneself an ability to control the visibility of any posts one was tagged in. Meanwhile, the sharing strategies characterize all possible actions that allow users to control the visibility of items posted by them to others. The fourth group, searching, signifies the permission users could grant to Facebook by allowing other people to search their profile via Facebook search utility or general public search engines. Lastly, filtering were strategies one used to set preference to posts made by others as well as preferences in accepting new friend requests.

Table-3. Privacy Strategies on Facebook.

Action: Security
- I deactivate my Facebook accounts every now and then. - I have strengthened my login password. - I added security question to my Facebook account. - I enabled secure browsing. - I generated specific passwords for applications. - I enabled login notifications. - I customized which applications and features can send notifications to my email.
Action: Tagging
- I untag myself from images and/or videos and/or messages posted by my friend. - I review all the tags and posts my friends made prior to displaying them on my Wall. - I disabled Facebook from suggesting my face in photos for tagging.
Action: Sharing
- I provided fake or inaccurate information to restrict people I don't know from gaining information about me. - I excluded personal information to restrict people I don't know from gaining information about me. - Certain friends on my Facebook only have access to limited profile. - I deleted messages posted on my Facebook Wall to restrict others from viewing/reading them. - I send private messages instead of posting messages to a friend's Wall to restrict others from reading them. - I customized which friends are allowed to view particular contents (e.g. Wall posts, photos, notes, etc.). - I limit the meaning of my messages so that only certain friends could understand them. - I customized who can see who are my friends, and also groups of friends (e.g. family). - I restricted who can read messages that friends posted to my Wall. - I did not share my photo albums with people who do not use Facebook. - I change my default privacy settings every now and then. - I view my profile from other's view after I changed my privacy settings. - I limited certain friends from having access to old posts on my Wall. - I personalized which information I share with applications. - I customized which information about me that friends can share with the applications they used.
Action: Searching
- I permit people on Facebook to search for my profile. - I give permission for people on the Intenet to search my Facebook profile using public search engines.
Action: Filtering
- I blocked few friends from contacting me and accessing my Facebook profile. - I segmented my friends into several lists. - I prevent some Facebook applications (e.g. games) from publishing to my Wall. - I filtered my News Feed by a specific friend or friend lists. - I filtered my News Feed to see specific types of stories only. - I edited my general preference (e.g. most recent posts, etc.) on News Feed to customize the posts I see. - I added a person or application that I have hidden back to my News Feed. - I removed a post and prevented all future stories from a person/application. - I only accept new friends if I know them in-person offline. - I only accept new friend requests if we share mutual friends. - Prior to accepting new friend requests, I scan their personal profile.

Data Collection

Prior to a large-scale data collection, we piloted this survey online from October 18, 2011 until November 17, 2011 using non-probabilistic convenient sampling [43]. Only Facebook users were invited to participate in the survey. The online survey was hosted on the commercial Smart Survey system. 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 University College London (UCL), Computer Science (CS) departmental mailing lists and electronic research subject pool system of UCL Psychology Department.

RESULTS

Demographics

139 respondents completed the pilot survey. According to [44], this sample size is sufficient for pilot studies in order to ensure the benefits of central limit theorem [45] applied. Respondents ranged in age from 18 to 54 years of age. Data analysis was performed using SPSS version 12.

Commonly Used Privacy Strategies

In order to find answers for our first research question, we used multiple response analysis to identify the most common 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.

Managing Personal Profile Visibility

Table-4. Personal Profile Visibility.

Privacy Strategies	Yes Responses (Count)	% of Cases
I excluded personal information to restrict people I don't know from gaining information about me.	79	57.2%
Certain friends on my Facebook only have access to limited profile.	77	55.8%
I send private messages instead of posting messages to a friend's Wall to restrict others from reading them.	113	81.9%
I customized which friends are allowed to view a particular content (e.g. Wall posts, photos, notes, etc.)	73	52.9%
I did not share my photo albums with people who do not use Facebook.	95	68.8%
I prevent some Facebook applications (e.g. games) from publishing to my Wall.	90	65.2%
I permit people on Facebook to search for my profile.	71	51.4%
I view my profile from other's view after I changed my privacy settings.	85	61.6%
I review all the tags in photos and posts my friends made prior to displaying them on my Wall	69	50.0%

Table-4 above shows the most common privacy strategies were used to limit access to certain audience for a set of personal information shared on Facebook. The need to limit the visibility of this information by imposing some access boundaries is probably driven by the norm of "appropriateness" and the norm of "distribution" of information flow; two privacy concepts which were devised by Nissembaum [46].

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 this norm when Facebook applications published on users' Wall about their activities when they used that application. In order to gain control over these applications, 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 breaches by other people based on user's expectations of what are appropriate and acceptable. For example, "tagging" is an efficient and convenient method of sharing a photo with the people in it. Although this goes against offline social norms [22] , this feature reduces the control that people have over the sharing and distribution of their own pictures.

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-5 below were commonly employed by Facebook users for managing their personal networking boundaries. 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-5. Personal Networking Boundary.

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

Managing Personal Privacy Awareness

Table-6. Personal Privacy Awareness.

Privacy Strategies	Yes Responses (Count)	of Cases
I customized which applications and features can send notifications to my email	88	63.8%
I change my default privacy settings every now and then	72	52.25%

Table-7 above lists the most used privacy strategies to manage privacy awareness. The results show that users did keep track on what was happening on Facebook and how the changes made by Facebook might have impacted their privacy. This finding is further 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.

The Relations between Privacy Strategies and Perceived Benefits

Using point-biserial correlation analysis between the commonly used privacy strategies and the items of perceived usefulness of Facebook, we presented answers for our second research question by summarizing the significant correlations. We found that private messaging was negatively correlated with the use of Facebook as a medium for promoting products (r = -.174, $p < 0.05$), whereas positive correlation was observed for publicizing events (r = .191, $p < 0.05$). This relation may suggest that private messaging on Facebook might not be useful for product commercialization, but it would be an effective tool for disseminating private events. We also found that users who occasionally modified their defaults privacy settings have tendency to use private messaging as well. This behaviour was observed probably due to the stability of privacy protection in private messaging in comparison to other social features such as timeline and group. As we have noted from literature and our experience in using Facebook, there were loopholes in the design of those features that could not guarantee protection of privacy as expected by users for the information shared [10].

Users who found Facebook was useful for revealing their thoughts and influencing others' views about certain issues were positively correlated to customizing the audience for each of their posts. This observation suggests that certain users value Facebook as an important medium to communicate and discuss ideas and opinions of certain issues to their intended audience. Due to this importance, these users may be very selective in terms of who can access what they post on their Facebook timeline, as well as whom they befriend with on Facebook by scanning the profiles of new friends requests. In addition, users who used Facebook to influence others about certain issues were also found to expose more personal information on the site (r = -.178, $p < 0.05$ for information exclusion). This behaviour is supported by the finding from [22][47].

Users who scanned profiles prior to accepting new friend requests also found that Facebook was useful for reinforcing their values on certain issues as well as meeting people. This may suggest that by being able to view personal profiles of the requesters prior to adding those requests, this strategy in some way serves as an opportunity for Facebook users to meet many other users on Facebook. While users who love using Facebook to reinforce their own values, this ability would allow them to be selective in terms of whom they choose to befriend on the site.

From the analysis, we also discover positive correlations between the use of profile search and the ability to show information and find contact using Facebook. Users who enabled profile search might have tendency to reveal more personal information about them since the tool was seen as an effective way to find contact among Facebook users. This finding is further supported by [18][48].

We also divided all 139 respondents into two groups: the one who perceived Facebook to be not that useful (call hereafter as 'less useful') and the group that found Facebook to be useful (called hereafter as 'more useful'). We calculated the mean score for each respondent. Respondents having mean score less than the mean value (Mean = 3.17, STD = 0.74) belonged to the 'less useful' group, while those with mean scores higher than the mean value were assigned to the 'more useful' group.

For each group, we performed multiple regressions (stepwise) between the independent variable (i.e. the most popular strategies; entered according to the percentage, from the highest to the lowest), and the dependent variable (i.e. the level of usefulness). The result of the regression (R2 = .04, F (1, 2.69) = 4.99) indicated that in the case of the 'less useful' group, the strategy to scan personal profile prior to accepting new friend requests significantly predicted the degree of perceived usefulness of Facebook (β = .13, $p < .027$). However no privacy strategies were predicted for the 'more useful' group.

This result shows that users who perceived that Facebook is less useful for them tended to scan profile of those who requested to be their friends prior to accepting the requests. This may suggest that this group of users have a higher tendency to add those whom they know or at least, 'strangers with acceptable characters' into their friend list. Due to redundant interactions that took place in online as well as offline contexts, this group of users might perceived Facebook as an additional point of contact whenever necessary.

The Relations between Privacy Strategies and Concerns for Privacy Risks

We examined correlations between the commonly used privacy strategies and the perceived concerns over privacy risks on Facebook to find potential answers for our third research question. Our analysis shows that there were significant correlations between these two variables. We found that strategies that manage profile visibility (i.e. excluding information, limiting profile view, customize audience for posts) are positively correlated to users' concerns over information theft and the risk of being discredited. By revealing personal information on the site, it surely increases the chances of having irresponsible users to steal the information and use it for illegal purposes. Another risk that concerns users was rather specific to their inner-self or self-identity; revelations make users perceive that others could discredit them [14]. For example, revealing that one hates his colleagues at work might lead to negative perception in others towards one's character. Other users might interpret that remarks as reflections of one's attitudes about his or her job.

Users' concerns over the risks of misinterpretation, information leakage and broken relations were positively correlated with the strategy users used to limit profile visibility only to certain friends. For some users, this strategy might seem effective to avoid stigma risk such as false misinterpretation of the information users post on the site that may cause negative outcome. It might also be useful for some users to avoid from embarrassment when the information users share might leak to irresponsible people. In response to reducing the risk of breaking a relationship, this strategy also might be useful for some users. In addition, customizing audience for posts users made on the site was also positively related to users' concerns over the risks of information leakage and broken relations. Concern for information leakage was also positively correlated with restricting applications from users' profile pages. For some users, letting people know what applications they used on the site, such as games in particular, might rather be embarrassing. The posts made by applications on their profile pages were actions that mostly unwelcome by many users [49][50].

Other interesting observations from this analysis were the relations between the risks for hackers and potential to jeopardize one's job position. An increase concern for hackers might indirectly lead some users to customize audience for certain posts they made. Internet criminals, hackers in particular, are very good in manipulating personal information for illegal purposes. Meanwhile, limiting profile to certain friends might also help some users in managing different personas to different people. In terms of job, their positions might be compromised when users reveal private information. For example, although users intend to ask for advice about marital problems from friends, having subordinate in the list might shift the definition of roles in a way that undermines the expectations for each position [14].

On the other hand, negative correlation was observed between the use of profile search and users' concerns over hackers, identity theft, stalking, blackmail, information leakage, and misinterpretation. The increased use of profile search suggests lower concerns for those privacy risks. However, this strategy is deemed useful for users to networking with other users. This might suggest that the usefulness on this strategy on Facebook might overcome the concerns of these privacy risks.

In terms of perceived concerns for privacy risks, all respondents are divided into two groups: 'less concern' and 'more concern'. 'Less concern' respondents are those who have mean scores less than mean value of the mean scores (Mean = 3.07, STD = 1.06) while respondents of 'more concern' acquire higher mean scores than the mean.

The analysis shows that users who perceived higher concerns for privacy risks on Facebook have tendency to limit accessibility of their profile page only to selected audience, and disabled other Facebook users to search for them using profile search utility. This is supported by the finding from [51] where they found more than half of their respondents were concerned that some of their "friends" could inappropriately forward their personal information to some other persons. In addition to that finding, Aimeur et. al. also found that inappropriate uses that users fear include the download and transmission of the pictures present in their profiles, the fact that their identity and personal information may be revealed online without their consent, the copies or abuses of their intellectual properties, online threats, and the divulgation of their information by the social network sites' providers to other parties without their explicit consent.

Multiple regression analysis (stepwise) shows no significant correlations were predicted for the 'less concerned' group.

DISCUSSION OF RESULTS

This study looks into studying the privacy strategies that were commonly used by Facebook users, and determining their relations with perceived benefits and concerns for privacy risks experienced by Facebook users. Privacy strategies were commonly used by Facebook users to manage: (1) profile visibility, (2) networking boundary, and (3) privacy awareness. This finding suggests that social network sites in general, and Facebook in particular, should give more attention to provide assistance and educate their users on privacy settings of these categories.

Our finding also shows that privacy strategies on Facebook might either involve direct use or indirect use of the Facebook features. 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 were no recommendation utilities on Facebook interface to assist users as to whether to reject or accept a new friend request. To help making their decisions, users might 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. Thus, this finding is useful to formulate 'privacy tips' by using social-oriented features that could be useful for users in protecting their privacy on Facebook.

This pilot study also observed significant relations between privacy strategies and the benefit-risk assessments of Facebook. This initial finding will be useful to further our investigation in this area. This initial would potentially be useful in devising necessary intervention in educating Facebook users about creative ways in protecting their privacy. The intervention should focus on creating an environment where Facebook users could build flexibility in the use of privacy strategies by acquire appropriate skills in managing online risks while advancing their ability to use Facebook in a beneficial way.

LIMITATIONS AND FUTURE WORKS

Since convenience sampling [52] was used to sample our respondents, the generalization of our results to Facebook population must be made with care. Our pilot sample does not represent the overall distribution of Facebook population [53]. For the study to be significant and representative, a large-scale study would be conducted in the near future in order to 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 analyses on the demographics of our participants. We would recommend future investigations to specifically looking at how various demographic profiles affect: (1) the most commonly used privacy strategies and (2) the relations between the used of privacy strategies and benefit-risk assessments of Facebook.

There are also several limitations to using an online survey to study human attitudes and behaviors towards privacy. Using the survey method could present the problem of conveying insufficient and biased information. This is further supported by boyd and Marwick [38] 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 were collected using surveys might not always be consistent with actual privacy behaviors [32][54][55]. As people move through different levels of privacy experience during social interaction on social network sites, assessing these levels are complex and require understanding of users' psychology and behaviors. Users also often demonstrated 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 we might not include all possible privacy strategies used on Facebook. Our items for this variable were collated from literature published before August 2011. As Facebook keeps on changing its interfaces and privacy settings, certain privacy strategies may become obsolete by today, and new privacy strategies were implemented along the way. Therefore, certain survey items for privacy strategies variable might eventually be adapted, modified or removed from future survey studies.

CONCLUSIONS

Because of intensive privacy settings offered by Facebook, this study provides an initial insight on how these settings were used strategically by Facebook users in order to reap the benefits of sharing on Facebook while at the same time, minimizing risks on their privacy. This study has identified the most popular privacy strategies used by Facebook users, and their relations with perceived benefit of using Facebook and concerns on privacy risks from using the site. This initial finding should land us a credential insight about how Facebook privacy settings have been used to support users in achieving their needs. Privacy designers would be able to take advantage by knowing how users have creatively adopted certain privacy settings to achieve certain personal purposes on Facebook. This serves as an opportunity to design interventions that could effectively educate users about the implications on using certain privacy settings on Facebook.

REFERENCES

[1] eBizMBA. 2015. Top 15 Most Popular Social Network Sites | August 2015. Retrieved August 30, 2015, from: http://www.ebizmba.com/articles/social-networking-websites

[2] Facebook. 2015. Facebook Newsroom. Retrieved August 30, 2015, from: http://newsroom.fb.com/

[3] J. Lewis. 2011. Facebook Faces EU Curbs on Selling Users' Interests to Advertisers. Retrieved August 30, 2015, from: http://www.telegraph.co.uk/technology/facebook/8917836/Facebook-faces-EU-curbs-on-selling-users-interests-to-advertisers.html

[4] C. Mccarthy. 2010. Do Facebook's new privacy settings let it off the hook?. Retrieved August 30, 2015, from: http://www.cnet.com/news/do-facebooks-new-privacy-settings-let-it-off-the-hook/

[5] M. McKeon. 2010. The Evolution of Privacy on Facebook. Retrieved August 30, 2015, from: http://mattmckeon.com/facebook-privacy/

[6] K. Opsahl. 2010. Facebook's Eroding Privacy Policy: A Timeline.

[7] E. Barnett. 2011. Facebook in New Row Over Sharing Users' Data with Moderators. Retrieved August 30, 2015 from: http://www.telegraph.co.uk/technology/facebook/9119090/Facebook-in-new-row-over-sharing-users-data-with-moderators.html

[8] J. Grimmelmann. 2009. Saving Facebook. Iowa Law Rev. Vol. 94, pp. 1137–1206.

[9] J. Grimmelmann. 2008. Facebook and the social dynamics of privacy. Retrieved August 30, 2015, from: http://www.ciberdemocracia.es/recursos/textosrelevantes/facebook.pdf

[10] danah boyd and A. E. Marwick. 2011. Social Privacy in Networked Publics: Teen's Attitudes, Practices and Strategies. Keynote speech for A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.

[11] danah boyd. 2010. Living Life in Public: Why American Teens Choose Publicity Over Privacy. Proceedngs of Association of Internet Researchers (AOIR 2010). Gothenburg, Sweeden.

[12] Y. Feng and W. Xie. 2014. Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with

privacy-protecting behaviors. Journal of Computer in Human Behavior. Vol. 33, pp. 153–162.

[13] C. De Rosa, J. Cantrell, A. Havens, J. Hawk and L. Jenkins. 2007. Sharing, Privacy and Trust in Our Networked World: A Report to the OCLC Membership. OCLC Online Computer Library Center Inc., Dublin.

[14] M. Chew, D. Balfanz and B. Laurie. 2008. (Under)mining Privacy in Social Networks. Web 2.0 Security and Privacy 2008 in 2008 IEEE Symposium on Security and Privacy. Oakland, California.

[15] K. Strater and H. R. Lipford. 2008. Strategies and struggles with privacy in an online social networking community. Proceedings of the 22nd British HCI Group Annual Conference on People and Computers Culture Creativity Interaction. Vol. 1, pp. 111–119.

[16] N. B. Ellison, C. Steinfield and C. Lampe. 2007. The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites. Journal of Computer Communication. Vol. 12, No. 4, pp. 1143–1168.

[17] S. Petronio. 2002. Boundaries of Privacy: Dialectics of Disclosure. State University of New York Press.

[18] A. Westin. 1967. Privacy and Freedom. New York Atheneum.

[19] K. Raynes-Goldie. 2010. Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook. First Monday Journal. Vol. 15, No. 1.

[20] J. Hart, C. Ridley, F. Taher, C. Sas and A. Dix. 2008. Exploring the facebook experience: a new approach to usability. Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges. pp. 71–474

[21] P. Niland, A. C. Lyons, I. A. N. Goodwin and F. Hutton,. 2014. Friendship Work on Facebook : Young Adults Understandings and Practices of Friendship. Journal of Community & Applied Social Psychology. Vol. 25, No. 2, pp. 123-137.

[22] S. Z. Ibrahim, A. Blandford and N. Bianchi-berthouze. 2012. Privacy Settings on Facebook : Their Roles and Importance. Proceedings of the 2012 IEEE International Conference on Green Computing and Communications. pp. 426 – 433.

[23] F. Stutzman, R. Capra and J. Thompson. 2011. Factors Mediating Disclosure in Social Network Sites. Journal of Computers in Human Behavior. Vol. 27, No. 1, pp. 590–598.

[24] F. Stutzman, R. Gross, and A. Acquisti. 2012. Silent Listeners : The Evolution of Privacy and Disclosure on Facebook. Journal of Privacy and Confidentiality. Vol. 4, No. 2, pp. 7–41.

[25] Facebook. 2015. Facebook Help Center. Retrieved August 31, 2015, from: https://www.facebook.com/help/

[26] danah boyd and E. Hargittai. 2010. Facebook Privacy Settings: Who Cares? First Monday Journal. Vol. 15, No. 8.

[27] A. L. Young and A. Quan-Haase. 2009. Information Revelation and Internet Privacy Concerns on Social Network Sites : A Case Study of Facebook. Journal of Public Policy. Vol. 5, pp. 265–274.

[28] E. Christofides, a. Muise, and S. Desmarais. 2011. Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults. Journal of Social Psychological and Personality Science, Vol. 3, No. 1, pp. 48–54.

[29] E. Babbie. 2011. The Basics of Social Research. Belmont, USA: Cengage Learning.

[30] R. Hill. 1998. What Sample Size is ' Enough' in Internet Survey Research? Interpersonal Computing and Technology: An Electronic Journal for the 21st Century. Vol. 6, No. 3, pp. 1–10.

[31] J. T. Roscoe. 1975. Fundamental Research Statistics for the Behavioral Sciences. Michigan, USA: Holt, Rinehart and Winston.

[32] P. Kline. 2000. Handbook of Psychological Testing. 2nd Edition. London, UK: Routledge.

[33] H. Nissenbaum. 2004. Privacy as Contextual Integrity. Washington Law Review. Vol. 79, No. 1.

[34] J. Rui and M. A. Stefanone. 2013. Strategic self-presentation online: A cross-cultural study. Journal of Computers in Human Behavior. Vol. 29, No. 1, pp. 110–118.

[35] E. Christofides, A. Muise and S. Desmarais. 2009. Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? Cyberpsychology and Behavior. Vol. 12, No. 3, pp. 341–345.

[36] A. Acquisti, R. Gross, P. Golle and G. Danezis. 2006. Imagined communities: awereness, information sharing, and privacy on the Facebook. Proceedings of the 6th International Conference on Privacy Enhancing Technologies, pp. 36–58.

[37] A. N. Joinson. 2008. ‘ Looking at ’, ‘ Looking up ’ or ‘ Keeping up with ’ People ? Motives and Uses of Facebook. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1027–1036.

[38] N. N. Bazarova. 2012. Public Intimacy: Disclosure Interpretation and Social Judgments on Facebook. Journal of Communication. Vol. 62, No. 5, pp. 815–832.

[39] E. Aimeur, S. Gambs and A. Ho. 2009. UPP: User Privacy Policy for Social Networking Sites. Proceedings of the Fourth International Conference on Internet and Web Applications and Services. pp. 267-272.

[40] W. M. K. Trochim. 2006. Nonprobability Sampling. Retreived August 30, 2015, from: http://www.socialresearchmethods.net/kb/sampnon.php

[41] Facebook. 2015. Company Info. Retrieved August 30, 2015, from: http://newsroom.fb.com/company-info/

[42] M. Taddicken. 2014. The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. Journal of Computing and Communication. Vol. 19, No. 2, pp. 248–273.

[43] G. Blank, G. Bolsover and E. Dubois. 2014. A New Privacy Paradox: Young People and Privacy on Social Network Sites. Oxford Internet Institute.

[44] Q. Hu and S. Ma. 2010. Does Privacy Still Matter in the Era of Web 2.0? A Qualitative Study of User Behavior towards Online Social Networking Activities. Proceedings of the Pacific Asia Conference on Information Systems (PACIS).