USERS’ PERCEPTIONS ON FACEBOOK’S PRIVACY POLICIES

1Zainab Asif, 2Mamuna Khan

Department of Computer Science and Information Technology, Jinnah University for Women, 5-C, Nazimabad, Karachi, Pakistan

Email: 1znbasif@gmail.com, 2mamuna.khan@gmail.com

ABSTRACT

SNS are becoming increasingly popular in almost every age group. People are willing to get socially connected to friends, colleagues, coworkers, family members, groups, natives and even to people whom they are not on familiar terms with. This intensifying popularity of social networking sites and people’s enthusiasm and involvement towards them is giving rise to many security concerns. As people share everything and anything on these sites, they themselves are risking the odds. Generally, social networking sites have privacy policies that users can configure as per requirement of each resource. These privacy policies contain all the vital and crucial information that users might need to be aware of prior to sharing their information. Unawareness of these privacy policies and settings results in exposure of users’ private data. Our research presents the study that people are ignorant of such privacy policies and settings, and even if they are conscious and they’ve read them, they hardly understand their effect. We have focused on Facebook’s privacy issues and their impact because its participants are dramatically growing. It defines privacy either as a private/public contrast or in terms of a network of “friends”, in which all “friends” are created equal and all relationships are reciprocal. It does not provide any mechanisms to specify the users’ privacy preferences for the usage done by third party applications on their personal data. We argue that even the computer science graduates have least idea regarding information disclosure by Facebook. To support our argument, we have conducted a survey which is rooted on minimal understanding of loosely defined privacy policies and settings of Facebook. For this, we have composed and evaluated a set of hypothesis that is conceived on the basis of Facebook’s privacy policies and settings and by observing various Facebook profiles. The survey participants selected, are between the age group of 18 to 32 and are categorized as either computer graduates or general students. We have selected this set of population, because it is considered that they have the most knowledge pertaining to information technology and its practices. We have also contributed few suggestions on privacy policies for new users by exploring knowledge of existing policies. The objectives of this research are twofold: (1) To study the amount and type of information disclosed by Facebook, its consented parties and other Facebook users (2) To compare our findings with regard to the hypothesis that creates a foundation as to why people do not properly organize their Facebook privacy settings.

Keywords: Social Networking Sites (SNS), Facebook’s privacy settings and policies.

1. INTRODUCTION

Social networking is becoming a necessity day by day. It is a phenomenon that is exploited by SNS, which strive to transform relationships between people and groups of people which already exist into an online network which can be traversed and exploited [4]. These sites have now transformed into social networking services [4]. And, people are eagerly signing up to these social websites. But apart from the attraction they have, there are also some hidden threats that they possess.

In SNS, people are free to decide what they share themselves but they cannot control the content others post about them [1]. They allow users to present a profile of them through a long list of very detailed information [5]. As, not everything is to be shared with everyone [7], Social networks will collect data for any purpose, or for a single specific purpose, then later reused for any purpose [4] that can be used by spammers to obtain new email addresses. Privacy leakage is one of the biggest problems of social networking as many users do not always understand the implications of revealing personal information online. [3]. And, Information is leaked because of the design of privacy controls of the SNSs [5]. All of the privacy policies involved do not have clear statements with regards to the retention of the data provided [4]. Even if the user seeks out the policy, it could be too long or written in terms that are difficult to understand thereby encouraging the user not to bother reading [2]. And then the user might assume there data may be kept private, and therefore not seek out the privacy policy [2]. Users need to be informed in easily accessible privacy statements that are easy to understand - especially by young adults who make up a substantial proportion of their users [2]. Because, information is gathered from them without their knowledge to market products of organizations partnered with the SNS [2].

2. FOCUS OF STUDY

This research paper presents the study that complicated and tricky privacy policies are hard for the users to understand and even if they understand them, they are hardly aware of the correct effect. As indicated in the abstract, the objective of this paper is two-fold: (1) To study the amount and type of information disclosed by Facebook, its consented parties and other Facebook users (2) To compare our findings with regard to the hypothesis that
creates a foundation as to why people do not properly organize their Facebook privacy settings. Our first objective gave us the basis to accomplish our second objective.

3. RESEARCH APPROACH
The participants chosen for this research are distinguished as computer graduates and computer literates. To distinguish the awareness of both set of users we created and evaluated a set of hypothesis that is conceived on the basis of Facebook’s privacy policies and settings and by observing various Facebook profiles and other researches in this background. We collected our data using online survey forms.

4. ANALYSIS AND DISCUSSION
To verify our first objective, we went through the privacy policy of Facebook and sought many other research papers in this subject matter. The information gathered in the first objective, facilitated in verifying the hypothesis in the second objective. The following are the list of hypothesis, preceded by the discussion.

4.1 Hypothesis
1. People do not read privacy policies
2. People read privacy policies but
   a. They do not understand the vocabulary
   b. They are not sure about the effect of the setting
3. People willingly allow third parties to access their information because they believe that they are owned and operated by the Social Networking Site.
4. People assume that by making their profile private, their information can never be shared
5. People do not know how their use of SNS can list them in search engines
6. People believe that by deleting certain information (e.g. photos, tags etc) or by deactivating the account, will remove their content permanently
7. People do not verify their friends requests
8. People believe that by blocking a user, it will restrict the blocked user from tracing them

To validate our hypothesis, we are putting forward some arguments that will present the results by comparing the information provided in Facebook’s policy with our research’s outcome.

Argument 1:
As stated in Facebook’s privacy policy, “We do not own or operate the applications or websites that you use through Facebook Platform (such as games and utilities)”1. That means that when users use applications and websites through Facebook, they are actually letting their information available to someone other than Facebook.

Further on this context, Facebook is saying “You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules”1.

Have you ever read the privacy policies of any application (e.g. FarmVille) you used on Facebook?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>87.9</td>
</tr>
</tbody>
</table>

Figure A

To evaluate whether users know about this policy, we asked our participants that whether they have read the privacy policy of any game or application they have used on Facebook. 87.9% of the respondents said ‘NO’. (As depicted in Figure (a)

To argue more on this context, Facebook is saying that “When you connect with an application or website it will have access to General Information about you. The term General Information includes you and your friends’ names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting”1.

Have you ever signed in to any site by using your Facebook account?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.2</td>
<td>50.8</td>
</tr>
</tbody>
</table>

Figure B

For this, we asked our respondents that whether they have signed in to any site by using Facebook (As shown in Figure (b)). And 49.2% answered ‘YES’.

1 http://www.facebook.com/policy.php
This argument proves that our hypothesis 3 is true and it can be evaluated as no matter how much users be concerned about the privateness of their personal information, their information is revealed to third parties anyhow. Because Facebook itself is saying that “Sometimes we share aggregated information with third parties to help improve or promote our service. But we only do so in such a way that no individual user can be identified or linked to any specific action or information”. And Facebook itself is disqualifying the above statement by saying that “Service providers may have access to your personal information for use for a limited time, but when this occurs we implement reasonable contractual and technical protections to limit their use of that information to helping us provide the service”.

**Argument 2:**

To further define how many other ways Facebook discloses users’ information without their realization, we place our second argument that users reveal all their private and personal information to their ‘friends’. However, there is no guarantee that their friends have a private profile. On this issue, we are referring to a policy of Facebook which states that, “If your friend connects with an application or website, it will be able to access your name, profile picture, gender, user ID, and information you have shared with everyone”.

This argument is further verified by another policy which states that “The owner of a photo can still share that photo with people you’re not friends with”. Because in SNS, people are free to decide what they share themselves but they cannot control the content others post about them.

**Figure C**

To verify how many users are aware of this policy and how much data they have revealed to their friends, we asked our respondents about some of the settings they have applied on Facebook which included settings for ‘see your friends list, status and posts (Depicted as Setting 1 in Figure C)’ and for ‘photos and videos you are tagged in (Depicted as Setting 2 in Figure C)’. 88.9% of our respondents have allowed their friends to see their friends list, status and posts and 77.8% of our respondents have allowed their friends to see the photos and videos in which they are tagged.

This argument can be concluded as such that people share everything with their friends without any knowledge that their private profile or personal information is becoming public through their friends. Therefore, Hypothesis 4 = True.

**Argument 3:**

It is clearly stated by Facebook, “Your name and profile picture do not have privacy settings”. Nearly everyone stores their name [2]. Names extracted from social networks can be used to harvest email addresses as a first step for personalized phishing campaigns [3]. And Facebook is saying that ‘We allow other users to use your email address, to find you’.

This means that Facebook itself is providing your email address to phishers.

This puts our concern to another area that no profile is private. As Facebook is saying that “Information you’ve shared with everyone - as well as your name, profile picture, gender, networks, and username - could be seen by anyone on the internet”. And by internet it means that they can be searched on Google.

**Figure D**

We directly asked our respondents whether they have any knowledge that they can be searched on Google. And, 80.1% said No. This evaluates that these 80.1% (which includes 22% of the computer graduates) have not read the privacy policy. And surprisingly, out of these 80.1%, 63.8% of the respondents said they have read the privacy policy of Facebook. And this proves our Hypothesis number 5 as true.

To further verify our argument, we put our interest on how many users have set their Facebook settings visible to ‘Everyone’. For this we asked our users about some of their Facebook settings.
The finding of this study includes how many users have set their settings to ‘Everyone’ (As shown in Figure E). 40.7% have allowed ‘Everyone’ to search them on Facebook (As depicted as Setting 1 in Figure E) and 55.6% have allowed ‘Everyone’ to send them friend requests (As depicted as Setting 2 in Figure E). However, no users have allowed ‘Everyone’ to see their friend list, status, photos and posts (As depicted as Setting 3 in Figure E) and only 7.4% have permitted to ‘Everyone’ to comment on their posts (As depicted as Setting 4 in Figure E).

The above findings directed our concern on whether users know the correct meaning of the ‘Everyone setting’. To get to the bottom of our confusion, we asked our respondents that what they comprehend with the setting ‘Everyone’. 34.5% answered Everyone on the internet (out of which 30.1% are computer graduates), 50% answered Everyone on Facebook (out of which 6% are computer graduates) and 15.5% answered Everyone in your friends list (As depicted in Figure F).

This gives us a clear result that 60.5% of the respondents do not know about the ‘Everyone’ setting. Out of this 60.5%, 35.2% respondents said that they have read the privacy policy of Facebook. This brings us to another conclusion that out of these 60.5% users, 32.5% have not understood the correct effect of this setting (Thus, Hypothesis 2(b) = True).

**Argument 4:**

Another policy of Facebook, that gave rise to our fourth argument states that “Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users”. And on the other hand Facebook is disqualifying the above policy by assuring its users that “When you delete an account, it is permanently deleted from Facebook”. Both the policies itself are giving the idea that users might not understand them. But to confirm our argument we asked our respondents that whether deleting any information (e.g. Pictures or email address) or deleting the account removes their data from Facebook’s records.

**Argument 5:**

Our fifth is supporting our 7th hypothesis.

Just by looking at a person’s name and some personal information, people believe that it is the same person they know. They do not verify whether the account belongs to the same person. To prove our argument, we created a bogus account which imitated like it’s one of our department’s lecturer’s, and provided some of the work information we knew about her. Then we added some of our social group. Immediately, people accepted and we also received requests from other students apart from our class as well (people
added by just seeing the name and the mutual friends). At present, we have a total of 56 friends on that account (which includes other lecturers from the department and students).

**Argument 6:**

Our sixth argument is that people suppose that once they have deleted a user or removed their connection from a person, that person can never trace them. On this context, Facebook is saying that “Once you block someone, that person can no longer be your friend on Facebook or interact with you (except within applications and games you both use)”. To support our argument, we asked our participants that, if they block any user, will that person be able to trace them from any application they use on Facebook?

![If you block any user, will he/she be able to trace you from any application you use on facebook?](image)

**Figure H**

As predicted, 62.7% did not know about this policy. This results that our 8th hypothesis is true, because a user either block can have access to your information once you are socially connected with that person.

<table>
<thead>
<tr>
<th>No.</th>
<th>Hypothesis</th>
<th>Survey Question</th>
<th>Response</th>
<th>Conclusion</th>
</tr>
</thead>
</table>
| 1   | People do not read privacy policies | Have you ever read the privacy policy of Facebook? | Yes = 63.8%  
No = 36.2% | Hypothesis 1 = True, if these 63.8% people have read the privacy policy then they should know that no profile is private, as your name and profile picture do not have privacy settings. |
|     | Do you believe that your Facebook profile is private? | Yes = 58.6%  
No = 41.4% |  |
| 2(a) | People read privacy policies but they do not understand the vocabulary | Do you know that using Facebook means you are allowing your information to be transferred and processed in US? | Yes = 58.6%  
No = 41.4% | Hypothesis 2 = True, because people are not understanding the adverse effects of providing their information to legal authorities |
| 2(b) | People read privacy policies but they are not sure about the effect of the settings | What does Facebook mean by "Everyone"? |  
Everyone on the internet = 34.5%  
Everyone on Facebook = 50%  
Everyone in your friends list = 15.5% | Hypothesis 2(b) = True, as clearly 65.5% of the respondents do not know the correct consequence of the setting |
| 3   | People willingly allow third parties to access their information because they believe that they are owned and operated by the Social Networking Site. | Have you ever read the privacy policies of any application (e.g. FarmVille) you used on Facebook? | Yes = 87.9%  
No = 12.1% | Hypothesis 3 = true, as people do not know how and where third party applications share their information |
|     | Have you ever signed in to any site by using your Facebook account? | Yes = 49.2%  
No = 50.8% |  |
| 4   | People assume that by making their profile private, their information can never be shared | Settings to see your friends list, status and posts | Everyone = 0%  
Friends only = 88.9%  
Friends of Friends = 5.6% | Hypothesis 4 = true, because it is not guaranteed that a friend will have a private profile |
We also conclude that complexity of privacy settings and lack of control for his guidance and wisdom throughout the research. Next, we would like to acknowledge our teacher, our mentor Ms N. Shawoo without whom this piece of work wouldn’t be possible. She can find the goodness and intelligence in anyone and then help build upon that always in such a way that the growth always belongs to that person. Ms N. Shawoo may be one of the most scintillating speakers we have ever heard, but even more impressive is that she is perhaps the best listener we have ever met. By listening, and concentrating, on what someone is saying, and then engaging them through that person's viewpoint, one learns in ways that one cannot quite imagine.

Next, we would like to pay our gratitude to our parents, who suffered sleepless nights just because the lights were on when we were working on the system. Last, but not the least we are grateful to people who participated in our survey. Without whose generous cooperation, this research could not have been achieved.

REFERENCES


[3] Iasonas Polakis, Georgios Kontaxis, Spiros Antonatos, Eleni Gessiou, Thanasis Petsas, Evangelos P. Markatos,

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Hypothesis 5 = true, because people can be searched through their email addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>People do not know how their use of SNS can list them in search engines</td>
<td>Do you think your profile is being shared by google?</td>
<td>Yes = 19.9%</td>
<td>Hypothesis 5 = true, because people can be searched through their email addresses</td>
</tr>
<tr>
<td>6</td>
<td>People believe that by deleting certain information (e.g. photos, tags etc) or by deactivating the account, will remove their content permanently</td>
<td>By deleting any information (e.g. Pictures or email address) or deleting the account will remove your data from Facebook’s records?</td>
<td>Yes = 70.3%</td>
<td>Hypothesis 6 = true, as information is never removed from Facebook’s’ database</td>
</tr>
<tr>
<td>7</td>
<td>People do not verify their friends requests</td>
<td>A fake account was created</td>
<td>56 respondents added the account without verifying.</td>
<td>Hypothesis 7 = true</td>
</tr>
<tr>
<td>8</td>
<td>People believe that by blocking a user, it will restrict the blocked user from tracing them</td>
<td>If you block any user, will he/she be able to trace you from any application you use on Facebook?</td>
<td>Yes = 37.3%</td>
<td>Hypothesis 8 = true, because a blocked user can trace you through an application that is mutual to you.</td>
</tr>
</tbody>
</table>
“Using Social Networks to Harvest Email Addresses,”
ACM, 2010


