Case Study Of Comparing Security Features Of Facebook And Google Plus

Raniah M. Alsahafi

Abstract: The topic of cloud computing is becoming well known these days. It enables many services to be easily accessed in the internet in anywhere in the world. People are sharing their life events with their friends over the internet using several types of social networking sites such as Facebook, Twitter, My Space, Google Plus and so on. This lead to spread much valuable information and it becomes hard to prevent these information from leaking. This Study compare the security features of the most popular social network: Facebook and Google plus. It discusses major features and threats that face them. Users are the most important defense line whether they are using Facebook or Google Plus. They are the only one who know how much security and privacy that they need and control the amount of information that they can post, also who allowed to access their profiles. I have tested the possibility of some of these threats. Furthermore, I had our own experience to test their users' security awareness. Then, based on all of that, I have compared between them in terms of security and privacy. Finally, I present my point of view regarding the case study.

Index Terms: Cloud computing, Facebook, Google plus, Data privacy, security risks, social networking.

1. INTRODUCTION

Nowadays, social networking, which is part of the cloud computing, has become necessity in people's lifestyle. People are sharing their life events with their friends over the internet using several types of social networking sites such as Facebook, Twitter, My Space, Google Plus and so on. This causes huge amount of personal information to be spread over the internet, and it is hard to prevent them from leaking which is violating the privacy of the users and leading them to so many problems. In this case study, I have chosen two of the most popular social networking sites which are Facebook and Google Plus. I have discussed about their main security features and some of the threats and attacks that facing them. Also, I have tested the possibility of some of these threats. Furthermore, I had our own experience to test their user's security awareness. Then, based on all of that, I have compared between them in terms of security and privacy. Finally, I present our point of view regarding the case study.

2. FACEBOOK

Facebook is a very popular social networking site that makes users interact with their interests easily. In Facebook profile, users share their information such as name, age, phone number, photo and email address etc. Also, they can specify their school, courses and other information. This might lead the users to serious risks such as identity theft. In this part, I will discuss several security features, threats, and attacks regarding the Facebook

2.1 Security Features of Facebook:

A. Groups in Facebook

By default, Facebook provide 3 groups to maintain friends: public, friends and custom. The users can choose any group when they are sharing any post or photo. For public group the content will be shown to all whoever can access the profile. For "friends" option the posts or photos are visible only to the friends in the user's list. In fact, users can make their own groups like co-worker, college friends, and classmates etc. to share information. Thus, they can choose a custom group to share information with.

B. Securing the Privacy of Profile Contents

Facebook users can control who can see the information on their profile. Facebook provide the option to share the information with specific people or make it totally public. For example, users can make their phone number visible to their family members while date of birth is visible to their friends. Also, users' friends may send a request for relationship or photo tag which will appear in the user's profile. The users have options to approve or ignore that request. Thus, malicious posts can be blocked in the profile page. Again, the user can restrict the information on their profile depending on the groups that they have.

C. Manage Post Privacy

Users can choose a group who can see a specific post. This security features allow users to post confidential information with their family or friends easily without revealing it publicly or sharing it with other peoples in friend list.

D. Change Past Posts

Users can change past posts. In fact, there are two features that help to modify the past posts. Users can change what they wrote previously with the new edit option from Facebook. Again, users can change the privacy of past posts anytime with Facebook's new security feature. For example, the users may have shared something publicly and later they want to make it visible to limited number of friends. In this case, they can change the privacy setting for that particular post and share it with who they want.

E. Blocking Suspicious Accounts

Facebook automatically checks the new accounts for identity authentication. It checks the information that provided in the profile, the number of friend requests sent by the new user, the response of friend requests, the posts, and friends response for a certain time limit. If there were random and huge outgoing friend requests recorded for any account, Facebook automatically alert that user and blocks him/her from sending friend requests for a certain period. Moreover, Facebook blocks either new or old accounts if they were reported as harmful or suspicious by many users. Again, before any user tries to develop an application, Facebook will check the authenticity of him/her by requesting an SMS verification or a voice call. This restricts the chance of sending automatic friend requests by malicious programs.

2.2 Threats & Attacks of Facebook

A. Identity Threats

Users may not be aware of the safety of the personal information, and they put their personal information on their profile which make it easy to an adversary to steal their Identity. With those information, adversary can search the person's identity and he could use this for criminal purpose. Also, some users reveal their location and home address which can be used by an attacker to attack them physically.

B. Personal Information Leakage

Many Facebook users accept friends that they do not really know. In this case, an adversary can easily become a friend with the users and he/she can access to their confidential information such as date of birth, email address and phone number. The risk come from the fact that an adversary can perform phishing information and spamming email. Moreover, an adversary can use malicious script to invite friends.

C. Cross Site Scripting, Viruses and Worms

Facebook is also vulnerable to XSS attack due to the third part applications. This type of attack allows the owner of the third-party application to inject malicious code in the users profile, which can compromise the account, thus, make it easy to perform a phishing attack.

D. Threat From Friend List

If an adversary can add someone as a friend, then he/she can access the friends list of that person and send malicious links or requests to those friends in the list. The adversary can spread rumor and/or malicious applications to all who are in the friend list. This causes disturbance for the users and also makes the network and the server busy with unwanted data. Moreover, Facebook users are victim of clickjacking. By this attack users unknowingly click on a link and spread malware across the network. Attackers usually sends some interesting or innocent news on people's wall with a “like” button or “read more” link. When anyone clicks on that link, that malicious application will spread over all his/her friends list and they will all get the same link. Thus, this malicious application spread from a person's wall to thousands.

E. Intellectual Property Theft

Users upload their photos, videos, music on Facebook with an intention to share them with their friends. They can easily be victims of intellectual property theft in Facebook. This type of harm can come from both known and unknown people. Threat comes from known people when a user shares his/her information with friends only, but they misuse this intellectual property like photo or video as there is no strict copy write law for these kind of files. On the other hand, if the users have unknown people on their friend list they can have those photos, videos etc. and they can make misuse of it. This can also happen if the user does not have privacy restrictions with his/her profile and/or intellectual properties.

F. Unplanned and/or Changing Facebook Without Prior Notice

Facebook makes changes in its framework frequently without giving any prior notice or newsletter to its users. Sometimes it shows the changes with/without enough descriptions. Most of the users are not aware of the changes. They do not cope up the changes which cause privacy problems. In that case, a user may have set up his/her privacy settings and believes he/she is secure inside Facebook, but the changing rules disclose all his/her private information without letting him/her know. Sometimes even if the changes that have been made were shown in the user's profile, they are not interested enough to read the whole instruction. This also causes privacy problems.

3. GOOGLE PLUS+

Recently Google Plus become the most popular social networking site, since it was opened to the public on June 30th, and even before that. It attracts millions of users with its features, such as "Hang Out" beside other amazing features, and the number of accounts being created grows rapidly. One fact that we can't ignore is that the security and the privacy that Google Plus provide for the users is one of the main factors of this popularity. We are going to discuss Google Plus features [30,36] form security perspective.

3.1 Security Features:

A. Circles

The effective weapon that Google Plus is using to attract users. Apparently, the circles have solved the most annoying problem that is facing other social networking users. Being exposed to everyone you have as a friend even though they aren't friend in real life. Some of the users of other social networking sites tend to have two different accounts to deal with this problem, which is really bothersome. However, it seems that this problem is no longer exist with Google Plus, thanks to the circles. The basic idea behind circles, that users divide their friends/followers into several categories like what they usually do in their real life, for example: family, friends, work, etc. So, whenever they want to post anything or upload a picture, they can choose which circle is allowed to see their post or picture, they even can make it limited to one person. This will allow Google Plus users to control which piece of information being shared with whom exactly, which guarantee their privacy.

B. Locking Profiles

By default, Google Plus user's profile will be exposed publicly to everyone to see their pictures, personal information, posts, location, relationships, and so on, which completely break the privacy rule. This unless the users modified the setting so only their circles can view their profile.

C. Restricting Search Ability

Also, by default, Google Plus user's profile and posts will appear in search results of Google and other search engines. So, the users must change the "Search Visibility" setting if they don't want to appear in there.

D. The Visibility of User's Circles

Some users don't want their relationship with other users to be known to everyone. Simply, they only need to change the circle's viewing setting.

E. Commenting on Other User's Posts

Even though Google Plus users have a full control over their own profile's posts and comments, the appearance of their comments on other's profiles will depends on the other's privacy settings. So, they must keep that in their mind before posting any comment.

3.2 Threats & Attacks:

A. The Appearance on Other's Profile

What applies for "posting comments" above also applies here. Google Plus users have no control over what others might post about them in their profiles. For example, a user A might post some personal information about his friend user B on her/his profile, so user B's information is exposed, despite the fact that he/she is already choosing to make his/her information private. Well, this is more like a human problem, than technical problem, and it should be solved by agreeing in some terms of privacy with the users that people add to their circles.

B. Google Plus Real Name Policy

Google Plus policy is violating one of the most important basics of privacy which is identity. People tend to use nicknames or pseudonyms while using internet. They want to be able to do their activities freely without being recognized with their real names. Giving opinions about controversial topics, joining activities that are not approved by their families, getting rid of some stalkers, or even protecting themselves form bothersome threats, no matter what the reasons behind that are, those pseudonyms keep them secure. However, it seems like Google Plus goes against this, stating that they want to connect the real world with Google Plus. So, Google Plus enforce users to use their real names to use the services that they provide. They use very strict rules to enforce the real name policy. Here are some of these rules:

- Use your full first and last name in a single language (e.g. first name in English and last name in Arabic not allowed).
- Avoid using special characters in your name.
- Name once changed must wait 30 days before changing again.
- If your name is legit and still the Google Plus system doesn't accept, you'll see appropriate instructions of how to appeal.
- Once a profile is suspended, all services that are dependent on the profile won't be available (Google Plus, Buzz, Picasa, Reader). Only after correcting the name and submitting the appeal.
- When a profile is found in violation by the system, you'll have up to 4 days to correct the name before system triggers a suspension [2,14].

Google Plus take those rules seriously; there are many accounts has been suspended because the users violate some of the rules. There are some stories about users who used their real names but Google Plus still suspected that and suspended their accounts. Although Google Plus provide a field for pseudonyms, they will still be associated with the real names. Some users have no problem with that or even with using their real name, on the other hand, there are some who totally disagree with it, and they started complaining about it. Last month, washingtonpost.com stated that Google Plus is considering about relaxing the real name policy in the next following months [31].

C. Photograph's URL problem in Google Plus

Google plus let his users face a huge privacy issue by allowing anyone to view their photos as long as they have the direct URL for theses photos. That despite the privacy setting the user apply on the photos. The one who discover this vulnerability stats that it's not hard to get the exact URL, and there are several ways to get it such as:

1. A vulnerability in Google+ servers is discovered and abused to get the addresses of image files.
2. The prediction of the URL building algorithm and prediction of these URL's.
3. Conducting a Man in the Middle (MITM) attack to get the list of URL's while the intended audience is viewing the images. [17] And according to him, Man in the Middle attack has the strongest possibility to happen. So, he suggested to modify the Gmail setting for the "Browser Connection" and activate "Always use HTTPs". Activating this option will make the eavesdrop between Google Plus and the browser very difficult that it will be hard to apply the man in the middle attack to get the photo's URL. However, this method will work only if all the users who allowed to see the photos are using http to view it. We have tested this vulnerability. We have uploaded two pictures and set the privacy for one of them as public and the other one as private and send their URLs to other friends. We found that they were able to view the public picture even though they don't have a Google account. As for the private picture, they weren't able to view it, whether they used a Google account or not, Google Plus prohibited their access to the picture. That means Google Plus has already fixed this vulnerability.

D. Google +1 Button Threat

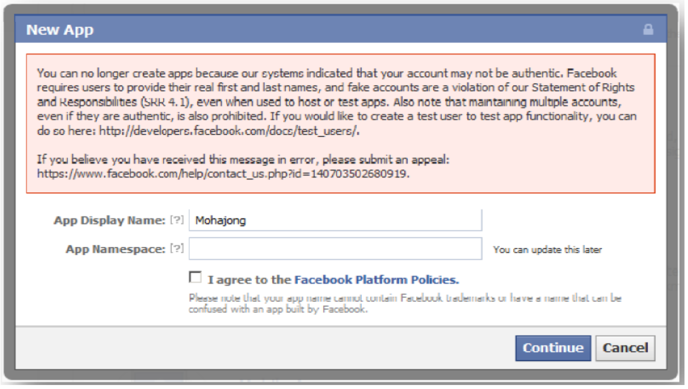
The Google +1 button is a way for users to share information publicly with the world. Google Plus use it to collect information about its users and their interests. Google Plus states that they might share aggregate statistics related to users' +1 activity with the public, their users, and partners, such as publishers, advertisers, or connected sites. For example, they may tell a publisher that "10% of the people who +1'd this page is in Tacoma, Washington." [12]. This might consider as privacy threat for some users, however, many users don't mind that.

4. EXPERIMENTS ON INFORMATION LEAKAGE IN SOCIAL NETWORKING

The security and privacy features that the social networking provide play main role in protecting the users. However, there is a fact that we can't ignore, these features might be useless sometimes; that depends on the user's self-awareness about how to secure themselves while using social networking. After I discussed and tested the security features, threats, and attacks in Facebook and Google Plus. I decided to test the users themselves and how aware they are in terms of security and privacy. We decided to do our experiment on Facebook since what applies for it applies also for Google Plus, and it's easier to test using Facebook since it's hard to make a fake account using Google Plus regarding their real name policy. We did two experiments, one related to the third-party application threat and the other one is related to self-security-awareness and leaking personal information

4.1 First Experiment: Third Party Application Threat on Facebook

As I discussed earlier, the third-party applications are one of the biggest threats facing Google Plus and Facebook users. I decided to develop a third-party application for Facebook and see how such a threat works on it. The goal is to have an access for the user's data, especially their sensitive data such as their e-mail address and phone number. In order to do this, we tried to develop a game; since games are popular in Facebook. The users have to give their personal information in order to accept it. So, we created a fake account on Facebook, and started to develop this game application. Also, we sent random friend requests to many users. However, while I was working on that, Facebook suspected the fake account and blocked it.So ,I no longer be able to access the account.



You can no longer create apps because our systems indicated that your account may not be authentic. Facebook requires users to provide their real first and last names, and fake accounts are a violation of our Statement of Rights and Responsibilities (SRR 4.1), even when used to host or test apps. Also note that maintaining multiple accounts, even if they are authentic, is also prohibited. If you would like to create a test user to test app functionality, you can do so here: http://developers.facebook.com/docs/test_users/.

If you believe you have received this message in error, please submit an appeal: https://www.facebook.com/help/contact_us.php?id=140703502680919.

App Display Name: [?] Mohajong

App Namespace: [?] You can update this later

□ I agree to the Facebook Platform Policies.

Please note that your app name cannot contain Facebook trademarks or have a name that can be confused with an app built by Facebook.

Fig. 1. *Facebook blocking our account and prohibited logging in.*

The Result of the experiment

From this experiment, we learned that Facebook has upgraded its security feature for this type of threat. And it will be harder to perform such an attack, but that doesn't mean that it's impossible.

4.2 Second Experiment: Self-Security-Awareness of

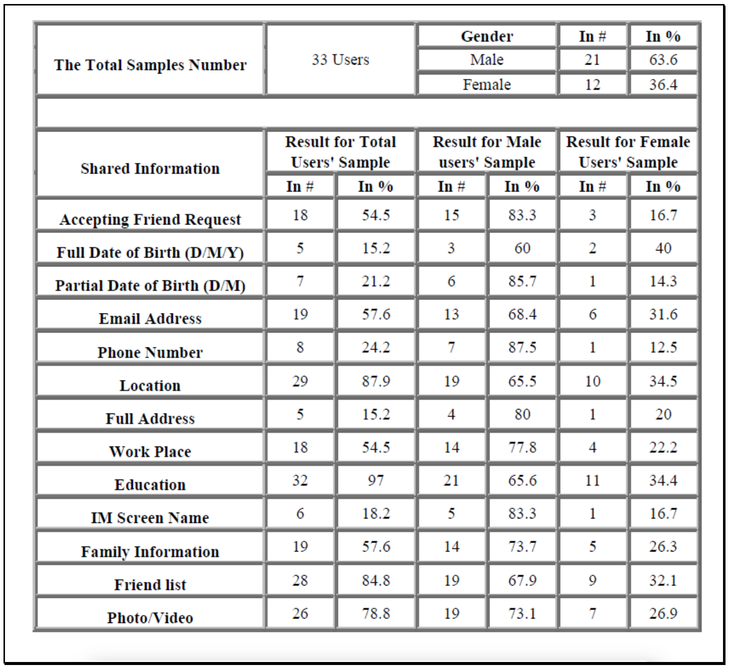
Since users may not be conscious of the privacy of personal information that revealed in Facebook profile that can lead to variety of security threats. To deal with social networking especially Facebook, users need to understand the possible risks and how to protect themselves against them. In Facebook, friends' list can bring several issues if users accepted adding people to their friends list even though they do not really know them personally. For this issue, I tested user's behaviors for accepting friend invitations, and how much of personal information those users revealed in their profile. I created both a male and a female fake Facebook accounts, and I sent random requests to both males and females users. I noted how many people have accepted those requests and revealed their personal information either to unknown people or publicly.

The Result of the experiment:

This experiment showed us that most people disclosed their confidential information to anyone. We can say that they are either lacking self-security awareness or they do not care about it even though they are aware of the problems that might face them in the future than female users.

TABLE 1

The Results of Self-Security-Awareness of Facebook Users



The Total Samples Number	33 Users		Gender		In #	In %
			Male		21	63.6
			Female		12	36.4
Shared Information	Result for Total Users' Sample		Result for Male users' Sample		Result for Female Users' Sample	
	In #	In %	In #	In %	In #	In %
Accepting Friend Request	18	54.5	15	83.3	3	16.7
Full Date of Birth (D/M/Y)	5	15.2	3	60	2	40
Partial Date of Birth (D/M)	7	21.2	6	85.7	1	14.3
Email Address	19	57.6	13	68.4	6	31.6
Phone Number	8	24.2	7	87.5	1	12.5
Location	29	87.9	19	65.5	10	34.5
Full Address	5	15.2	4	80	1	20
Work Place	18	54.5	14	77.8	4	22.2
Education	32	97	21	65.6	11	34.4
IM Screen Name	6	18.2	5	83.3	1	16.7
Family Information	19	57.6	14	73.7	5	26.3
Friend list	28	84.8	19	67.9	9	32.1
Photo/Video	26	78.8	19	73.1	7	26.9

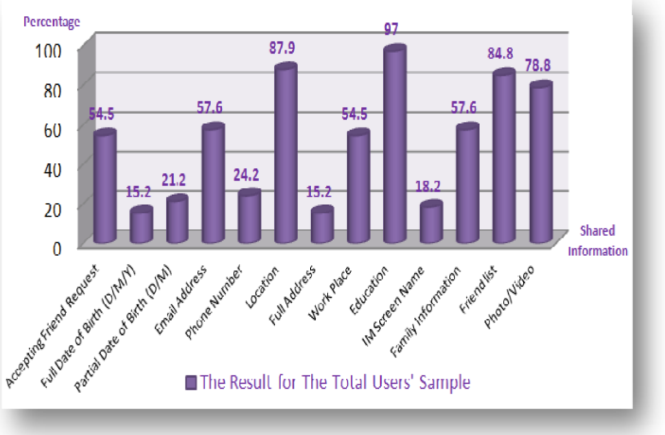


Fig.2. *Chart shows the total percentage of Facebook users sample who shared their personal information with unknown people*

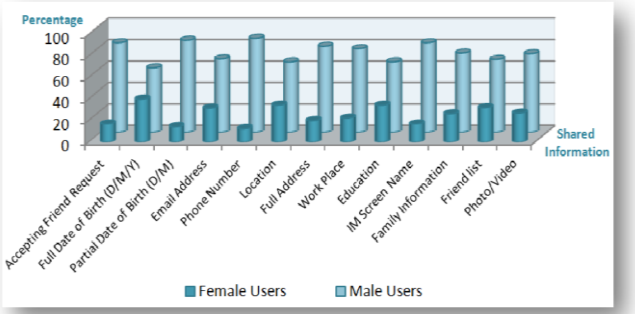
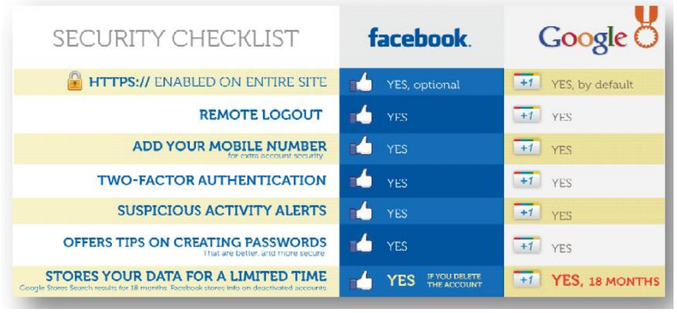


Fig.3. *Chart shows the percentage of Facebook male & female users sample who shared their personal information with unknown people.*

5. FACEBOOK VS. GOOGLE PLUS: SECURITY AND PRIVACY

After analyzing the security features, threats, and attacks of Facebook and Google Plus, and beside the result that I got from testing the user's awareness, I will compare between them in term of security and privacy. Veracode Application Security have provided excellent infographic [23] that compare between the two.

5.1 Security Checklist



SECURITY CHECKLIST	facebook.	Google
HTTPS:// ENABLED ON ENTIRE SITE	👍 YES, optional	+1 YES, by default
REMOTE LOGOUT	👍 YES	+1 YES
ADD YOUR MOBILE NUMBER for extra account security	👍 YES	+1 YES
TWO-FACTOR AUTHENTICATION	👍 YES	+1 YES
SUSPICIOUS ACTIVITY ALERTS	👍 YES	+1 YES
OFFERS TIPS ON CREATING PASSWORDS That are better, and more secure	👍 YES	+1 YES
STORES YOUR DATA FOR A LIMITED TIME Google Stores Search results for 18 months. Facebook stores info on deactivated accounts	👍 YES IF YOU DELETE THE ACCOUNT	+1 YES, 18 MONTHS

Fig.4.Security Checklist [32]

HTTPS

As social networking growing, more and more confidential information is transmitted via websites without any security layer. Social networking sites HTTPS instead of HTTP. That means the communication of increase the security. [24]. Both Facebook and Google Plus are using this protocol, however, Google Plus have the advantage over Facebook because it uses HTTPS by default, while Facebook make it option use it; keep in mind that some user don't really understand the difference between both protocols.

Remote Logout

Sometimes it happens that social networking users log in into their account from public computers or their friends' computers, and they forget to log out. This might cause problems for them, for example, leaking their personal information or the impersonating problem. However, this problem will no longer exists for Facebook and Google Plus users, since both provide the remote log out feature for their users which allow them to monitor their connection session and remotely log out from any active connection session [8,9].

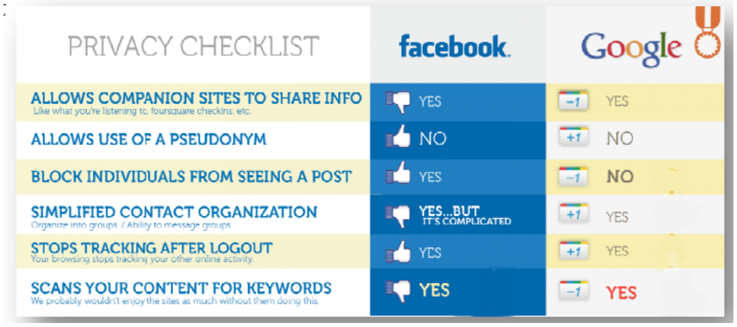
Mobile Number for Extra Security

Lately, both Google Plus and Facebook are using the mobile number to help the users to protect the security of their accounts. That's when the users log in from unrecognized or public computers that might be compromised with harmful software for example. So, instead of using their regular password they can use a one-time password that will be sent to their mobiles by Facebook or Google Plus [11].

Suspicious Activity Alert

Another great security feature that Google Plus and Facebook provide is detecting the suspicious behaviors and alert the users about them. For example, accessing the account from different geographical location, in such a case the users required to change their password to keep their account secure.

5.2 Privacy Checklist



PRIVACY CHECKLIST	facebook.	Google
ALLOWS COMPANION SITES TO SHARE INFO Like what you're listening to, foursquare checkins, etc.	👎 YES	−1 YES
ALLOWS USE OF A PSEUDONYM	👍 NO	+1 NO
BLOCK INDIVIDUALS FROM SEEING A POST	👍 YES	−1 NO
SIMPLIFIED CONTACT ORGANIZATION Organize into groups / Ability to message groups	👎 YES...BUT IT'S COMPLICATED	+1 YES
STOPS TRACKING AFTER LOGOUT Your browsing stops tracking your other online activity.	👍 YES	+1 YES
SCANS YOUR CONTENT FOR KEYWORDS We probably wouldn't enjoy the sites as much without them doing this.	👎 YES	−1 YES

Fig.5. Privacy Checklist [32]

Who Can Be Your Friend

Facebook got the point here. Basically, the users have the choice to accept or reject the friend's requests. On other hand, Google Plus users can't prevent others from adding them to their circles; which defiantly affects their privacy.

Allows Companion Sites to Share Info

One of the drawbacks of the social networking is allowing other websites and applications to access their personal information. This feature will give information about what are the users listing to, where are their locations, or even what kind of places the users usually visits. Unfortunately, this drawback exists in both user Facebook and Google Plus.

Allows the Use of Pseudonym

It's common for people to use a nickname or pseudonym when they join online communities nicknames and pseudonyms (false names) is banned in both Google Plus and Facebook. In order to fight spam and prevent the creation of fake profiles, using real names has become a most in these social networking sites. However, it seems that Google Plus is more strict in this point, since there are many users in Facebook are using pseudonym.

Block individual from Seeing a Post

Blocking people in social networking prevents unauthorized users from navigating unauthorized profiles to increase the privacy level. For instants, Facebook blocking property disallow others from seeing the individual profile that blocked them, or any related information about him/her. One other hand ,in Google Plus when someone block someone else, it's only preventing their posts to be shown in their pages. Someone block someone else, it's only preventing their posts to be shown in their pages.

Simplified Contact Organization

Although Google Plus (with its circles) and Facebook (with its lists) have their ways of organizing contacts, there are number of differences between them. Facebook Lists are hard to find and manage within the profile and tend to be difficult to be use for some people. Whereas, Google Plus circles are easy to find and fun to use and create. Also, the sharing property in Facebook does not reveal for the list members the other lists that sharing the same information with them. Having said that, Google Plus users can see the list of contact that sharing the same information with them. Moreover, there is no way for the users to see the content of the contacts who added them to their lists, but they did not add them back. Yet, Google Plus provide this feature in its circles [20]. So, it's fair to say that Google Plus got advantage over Facebook in this point.

6. CONCLUSIONS

As we all know that the nature of the social networking is about sharing data and information publicly. Most of the security burden fall on the service's providers. However, that doesn't mean that the users don't have any role in controlling their security and privacy. We believe that the users are the most important defense line whether they are using Facebook or Google Plus. They are the only one who know how much security and privacy that they need, and control the amount of information that they can post, beside control the people who allowed to access their profiles. Both Facebook and Google Plus are working endlessly to provide more features that handle the privacy and the security aspects; aiming to give their users a safe social networking experience. Which one is the best? Such a question is very hard to answer. Form what have we perceived through our research and the case study that we have done, we can say that Facebook and Google Plus are having an intense battle in terms of security and privacy that we can't clearly tell that one of them is better than the other one. The competition between the two is quite impressive. Whenever one of them launched a new security feature, it will only take few months or even weeks from the other one to announce developing the same feature and even in a way that is much more enhanced. For example, Facebook users have been complaining about their privacy; so they were impressed with the circles idea in Google Plus. However, Google Plus didn't got the chance to celebrate their victory of this feature for too long ; since Facebook added the smart lists feature few months later. To conclude, we can say that security and privacy are a necessity in the social networking world. And in order to reach the maximum level of both of them, both providers and users have to be accountable for their actions. In addition, both Facebook and Google Plus are keeping on upgrading their security features. Although there are some differences between these features, both have their advantages and disadvantages. Thus, deciding which one is the best between the two is undetermined and it depends on the user's point of view.

7. References

[1] A. Felt. "Defacing Facebook: A Security Case Study". Technical report, University of Virginia, July 2007.

[2] Google+ Real Name Policy Explained in Detail. Google+ News. Retrieved from http://google-plus.com/862/google-real-name-policy-explained-in-detail-invalid-profiles-may-be-suspended/, August 17, 2011.

[3] A privacy case study of Facebook users. Retrieved from http://www.architectingsecurity.com/2010/06/07/a-privacy-case-study-of-facebook-users/, June 7, 2010.

[4] A. Al Hasib, "Threats of Online Social Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009.

[5] The Most Common Security Threats on Facebook. Sick Facebook. Retrieved from http://sickfacebook.com/5-the-most-common-security-threats-on-facebook ,February 18, 2011.

[6] Basu.A."How To Configure Facebook Two-Factor Authentication. Make Tech Easier". Retrieved from http://maketecheasier.com/configure-facebook-two-factor-authentication/2011/06/17.June 17, 2011.

[7] Bill Pringle, Facebook security issues. Retrieved from http://billpringle.com/home/facebook.html,2011.

[8] D'Souza.E. Remote sign out and info to help you protect your Gmail account. Official Gmail Blog. Retrieved from http://gmailblog.blogspot.com/2008/07/remote-sign-out-and-info-to-helpyou. html#!/2008/07/remote-sign-out-and-info-to-help-you.html. July 7, 2008.

[9] Facebook Security. Forget to Log Out? Help is on the Way. Facebook. Retrieved from http://www.facebook.com/note.php?note_id=42513620076 . September 2, 2010

[10] Harvey Jones, Jos´ Hiram Soltren,"Facebook: Threats to Privacy".

[11] Opt-in Security Features. Facebook. Retrieved from http://www.facebook.com/help/?page=132501803490562 Facebook Help Center.2011.

[12] Google +1 Button Privacy Policy. Retrieved from http://www.google.com/intl/enUS/+/policy/+1button.html. (June 28, 2011).

[13] Google+ Privacy Policy. Retrieved from http://www.google.com/intl/en-US/+/policy/.November 7, 2011.

[14] Your name and Google+ Profiles. Retrieved from http://www.google.com/support/plus/bin/answer.py?hl=en&answer=1228271. Google (2011).

[15] Advanced sign-in security for your Google account. Retrieved from http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html.Google Blog. February 10,2011.

[16] Harpner.C,Major Google+ Security Flaw! Retrieved from http://blog.csharpner.com/2011/08/major-google-security-flaw.html.August 03,2011.

[17] Kirpininyeri. (Google Plus security – Scene 1. Retrieved from http://www.kirpininyeri.com/2011/07/google-plus-security-scene-1/. July 15,2011.

[18] Mandloi.A. (November 1, 2011). Prevent Google Plus Profile from Appearing in Search Engines. Retrieved from http://www.gtricks.com/google-plus-tricks/prevent-google-plus-profile-name-appearing/.

[19] C. Patsakis,A.Asthenidis. A.Chatzidimitriou." Social Networks as an Attack Platform:Facebook Case Study". Networks. ICN '09. Eighth International Conference on: 245-247. March, 2009.

[20] "What are the differences between Facebook's customizable friends lists and Google+ Circles?. Retrieved from http://www.quora.com/Google+-Circles/What-are-the-differences-between Facebookscustomizable-friends-lists-and-Google+-Circles.SQuora. (2011).

[21] Make Requests Through Google Servers Ddos. Retrieved from http://www.ihteam.net/advisory/make-requests-through-google-servers-ddos. (August 29, 2011).

[22] Distributed Denial-of-Service Attack (DDoS). Retrieved from http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack. June, 2001.

[23] S.Leitch, M.Warren."Security Issues Challenging Facebook".Edith Cowan University, Australian Information Security Management Conference.

[24] T.Sieber. "What Is HTTPS & How To Enable Secure Connections Per Default. Make UseOf". Retrieved from http://www.makeuseof.com/tag/https-enable-secure-connections-default/.August 25, 2011.

[25] P.Singh. "Ignore And Block People On Google Plus." Google Plus Blog. Retrieved from http://www.googleplusblog.info/2011/08/igrone-and-block-peolpe-on-google-plus.html. August 31, 2011.

[26] Facebook: The Privacy Challenge". Retrieved from http://www.sophos.com/en-us/securitynews-trends/security-trends/facebook.aspx. Sophos.2011.

[27] "Facebook users at risk of "rubber duck" identity attack. Retrieved from http://www.sophos.com/en-us/press-office/press-releases/2009/12/facebook.aspx. December 7, 2009.

[28] Squidoo. "Facebook Warning: Activities That Could Get You Banned". Retrieved from http://www.squidoo.com/facebook-bans.September, 2011.

[29] Swati. "Facebook adds some major Privacy Control Features: Is Google Plus in danger now?". Retrieved from http://www.buzzom.com/2011/08/facebook-adds-some-major-privacy-controlfeatures-is-google-plus-in-danger-now/.August 24, 2011.

[30] Swati. "How To: Protect your Privacy on Google+". Retrieved from http://www.buzzom.com/2011/07/how-to-protect-your-privacy-on-google/.July 26, 2011.

[31] H.Tsukayama. "Google Plus relaxing real name policy". Washington Post. Retrieved from http://www.washingtonpost.com/business/technology/google-plus-relaxing-real-namepolicy/.html. October 20,2011.

[32] Veracode. "Google vs. Facebook on Privacy and Security". Now Sourcing. Retrieved from http://www.veracode.com/resources/google-vs.-facebook-on-privacy-and-security.html. October, 2011.

[33] Wasil.G. How To Hide Your Facebook Profile From Search Engines. Vast 9. Retrieved from http://www.vast9.com/tech-tips/hide-facebook-profile-search-engines/.April 29, 2011.

[34] "How to Prevent Social Networks from Tracking Your Internet Activities. Retrieved from http://googleplus.wonderhowto.com/blog/prevent-social-networks-from-tracking-your-internetactivities-0130280/. October, 2011.

[35] Word Stream."Facebook Wall Of Shame (Infographic). Now Sourcing". Retrieved from http://nowsourcing.com/2011/10/19/facebook-fails-infographic/. October 19, 2011.

[36] "Guide to Taming Privacy Concerns Around Google+". Retrieved from http://blog.zonealarm.com/2011/07/privacy-concerns-around-google-plus.html. July 21,2011.