How Much Privacy We Still Have on Social Network?

Mafaisu Chewae[*], Sameer Hayikader[**], Muhamad Hairulnizam Hasan [***], Jamaludin Ibrahim[****]

[*] faa.izoon@gmail.com, [**] sameer797.kader@gmail.com, [***] redspira@gmail.com, [****] jamal55@gmail.com

Department of Information Systems, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia

Abstract- Recently, internet is one of the most efficient and effective ways to communicate and sharing the information especially in terms of social networking sites. With over billions of users connected through online social network and due to the popularity of social network sites, more people are concerning about the privacy and it has become an important issue. In this paper we will review how the current privacy plays on social network sites, analyze how personal information is being influenced by internet and social network, and also we will discuss how the privacy become a risk and how to employ security awareness to avoid privacy risk.

Index Terms- Privacy, Social Network, Threats, Privacy awareness, Risk factors

I. Introduction

Millions of internet users use social networking website to communicate with their friends, share their thoughts, photos, and videos. It’s critical for all computer users to be aware about computer security and privacy and to know what steps to take to defend against attacks. Social networking privacy issues have risen among users. As number of social networks is growing, the default settings share everything and what is important is that users have to set their privacy setting options to make their accounts more private. At the same time security attacks continue to be a major concern of all users. How to keep computers and social networking more secure and more private are the challenges that have been concern for every users. Not only because of the number of attacks but also because of the difficulties faced in defending against these attacks and threats. Online networks provide significant advantages both to the individuals and in business sectors. Many users provide information about themselves on social network which can be searched and hacked by the strangers. Thus, it raises privacy and security issues. Unfortunately many users are not aware of this.

II. LITERATURE REVIEW

Currently, in the era of advanced internet technology, Social Network becomes incredibly popular tool on the internet and becomes widely used around the world. It is powerful tool in any ages of people especially among teenagers and young adults in the propose of communication and self-expression [1], and it is easy mean of sharing information with other users who has a common interest such as photos, likes, dislikes, interests, relationship status, job details, current town details, political views, religious views etc. [2] [3] [4]. Unfortunately, though this technology most of users are not aware of the privacy risk associated whenever they shared sensitive information in the internet [4], so that privacy concern will be raised among those online interactions if their personal information has been shared to other people [3] [5].

According to consumer security risks survey 2014, is done by B2B International in conjunction with Kaspersky Lab shown that even using social networking is worldwide, but however there are minority of them understanding the risks of using social networking especially in terms of using mobile device to access the sites. Correspondingly, more than 78% of correspondents did not concern their information to be targeted by cyber-attacks or cyber-crime and they though that no any dangerous with any activities on their social network. The survey also found that one of ten has ever conversed to anonymous person about personal information, while 15% sending personal information which has not been exposed anywhere before through social network. Furthermore, 12 % of correspondents using public Wi-Fi to fill online account information, but only 18% of them who concerned that their personal information disclosure is excessive or not and 7% seriously considered their communicating through social networking is one of major factor which information will be lose [6].

Every social network sites ask users to accomplish a profile which contains privacy information including name, address, e-mail and so on. Through this information is claim to be danger which can be easily accessed by unexpected person [7] [8], but what is happening today, most of social network users tend to public real identity and post private information where privacy will be raised [9]. Accordingly, [3] [4] [7] [8] [10], they described that online social networking data is of great help to the researchers, analysts, and any kind of third party who has opportunity to mine and use data for particular purposes such as spamming, fishing, targeted advertising and so on [4]. This is because sensitive information and their interaction are stored in social OSN server are not always honest and transparent due to the nature of OSN allows third parties to collect and analyze easily [9].

Raji and her colleagues demonstrated that there are some principle privacy problems in social network like Facebook. For instance, Users used their real information to create an account profile to the rest of the Facebook users, The default privacy settings are not enough in Facebook, so users expose too much information to others users, Users do not change the OSN default privacy settings that are provided, and Sometime it is unavailable to adjust the privacy setting which is offered by Facebook such as the users can see the whole his or her shared information whenever users add his or her to be in friend list [9].

However, sometime there is a must to users to reveal personal information in particular reason, as demonstrated by [7]. They also illustrated that users have to reveal the personal information on social network in order to be effective and do this for maturing their identities. In reality, online communication can bring them to be intensive revelation compared to face to face communication. Furthermore, in the face of information of behavior of users are able to conceptualize as continuum which describes as information privacy protection behavior. This means information can disclose accurately in one side, but it is not for other sides. By the way, users can participate all and can protecting their personal information at the same time by partly disclosing of them.

III. RECENT SOCIAL NETWORK'S ACTIVITIES

It is not be denied that consuming of social networks (Facebook, Twitter, Google Plus, LinkedIn and Pinterest) are increasing considerably, people turn and trust them to share the information. However, there are still large number of user's online social network did not recognize that their information will be delved by anonymous person and did not concern enough about their privacy [7]. In the graph below shows the number how many billions and millions of people prefer social network sites in today world.

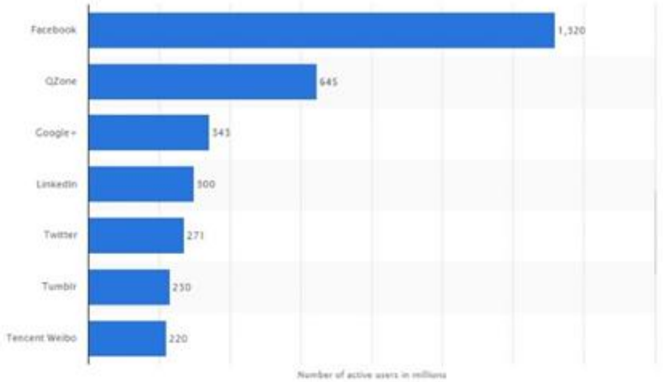
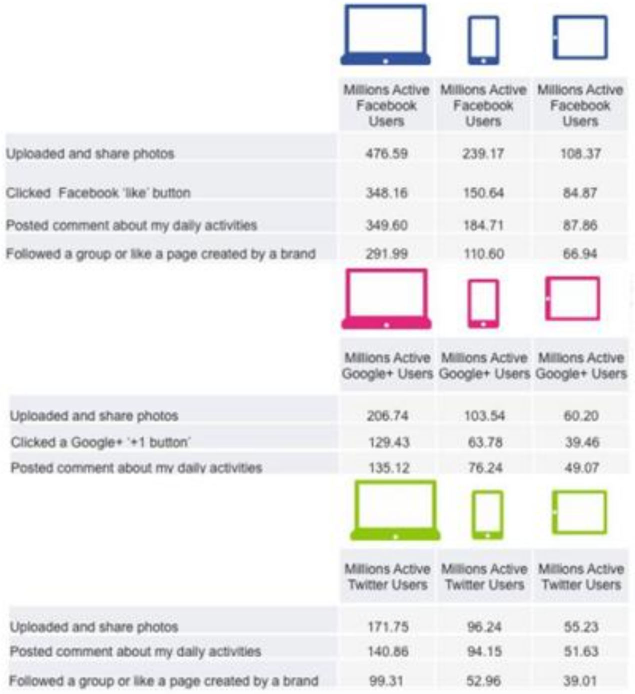


Figure 1: Number of Users on Popular Social Network sites [11]

Regarding to recent statistic of social networks worldwide usage above ranked by number of active users found in October, 2014, Facebook was the first social network to surpass billion registered accounts. Third-ranked Google+ had over 320 million monthly active accounts. Meanwhile, microblogging network Twitter had less than 300 million active users on their site [11].

Moreover, the statistic of social network activities in 2013 as show in figure 2 described that how activities were play in social network; uploading and sharing photos on Facebook is the most popular activities by achieving over 800 million active users, while Google+ and Twitter had about 370 and 323 million active users of uploading and sharing photo respectively. Furthermore, posting comment about my daily activities in Google+ and Twitter are not common as Facebook, which are only half of Facebook active users posted comment, while active users of posting comment about daily activities had only 361 and 286 million respectively [7] [12]. Correspondingly, more than 20% of Facebook users do not concern about privacy setting as possible [7], meanwhile the consumer security risks survey 2014 [6], shown that less than 20% of social network users concerned to the personal information will expose excessively or not.



	Millions Active Facebook Users	Millions Active Facebook Users	Millions Active Facebook Users
Uploaded and share photos	476.59	239.17	108.37
Clicked Facebook 'like' button	348.16	150.64	84.87
Posted comment about my daily activities	349.60	184.71	87.86
Followed a group or like a page created by a brand	291.99	110.60	66.94

	Millions Active Google+ Users	Millions Active Google+ Users	Millions Active Google+ Users
Uploaded and share photos	206.74	103.54	60.20
Clicked a Google+ '+1 button'	129.43	63.78	39.46
Posted comment about my daily activities	135.12	76.24	49.07

	Millions Active Twitter Users	Millions Active Twitter Users	Millions Active Twitter Users
Uploaded and share photos	171.75	96.24	55.23
Posted comment about my daily activities	140.86	94.15	51.63
Followed a group or like a page created by a brand	99.31	52.96	39.01

Figure 2: social network activities in 2013 [7] [12]

IV. PRIVACY CONCERNS WITH SOCIAL NETWORK'S SERVICES

The popularity of social networks service is not a secret anymore. With 1.35 billion users connected with Facebook, followed by 340 million with Google+ and 280 million on twitter, the phenomena has moved the way how people communicate from interpersonal communication into mass media communication[13]. They freely to talk to anybody regardless of their mutually know each other or not. However, the most controversial issue with regard to the social networks services is how genuine they keep the privacy in private. There are many possible ways that the privacy of a social network user's information can be compromised: publication of specific information on the network to unintended recipients due to poorly understood defaults, accidental data release, intentional use of private data for marketing purposes by the social networking site, court order, and so on [14].

While people keep talking about privacy, the issue of the borderline between public area and private area of social media space are still unclear. In some situation, users want their personal information to be known only by a small circle of close friends, and not by strangers. While in other scenario, they are willing to reveal personal information to anonymous strangers, but not to those who know them better, like their father or mother. Dwyer et al. have risen up a question on the relationship between Internet privacy concern and their willingness to share information and develop new relationship in [15]. They proposed the diagram to show the inter-relationship between privacy and trust.

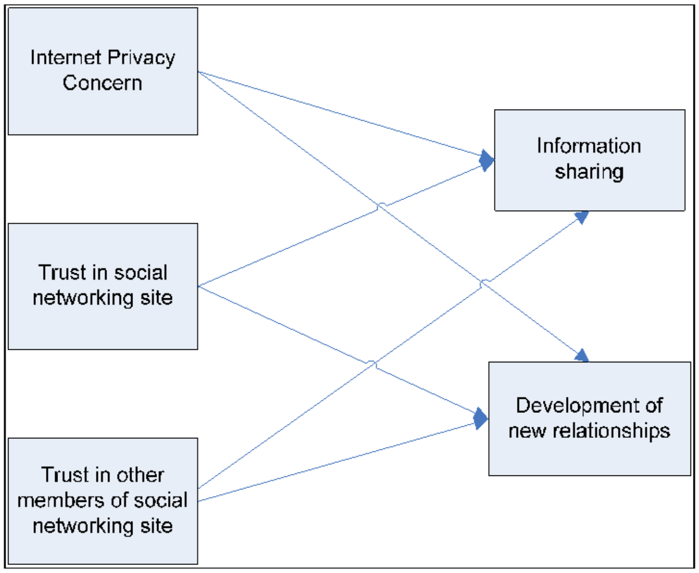
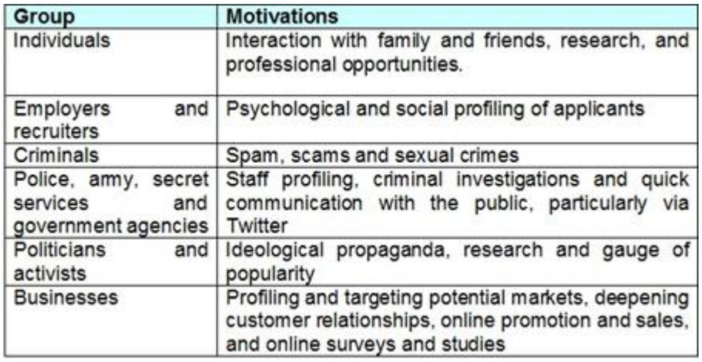

Internet Privacy Concern
Trust in social networking site
Trust in other members of social networking site
Information sharing
Development of new relationships

Figure 3. Privacy and trust model

The diagram shows that in order to develop new relationship some privacy need to be revealed in order to get trust from other party. However, the question here is that how much trust we can allocate for a new relationship and how trusted is the person that we are going to develop a relationship with?

The figure 4 shows the group of users and their motivational of using the social networks [16].



Group	Motivations
Individuals	Interaction with family and friends, research, and professional opportunities.
Employers and recruiters	Psychological and social profiling of applicants
Criminals	Spam, scams and sexual crimes
Police, army, secret services and government agencies	Staff profiling, criminal investigations and quick communication with the public, particularly via Twitter
Politicians and activists	Ideological propaganda, research and gauge of popularity
Businesses	Profiling and targeting potential markets, deepening customer relationships, online promotion and sales, and online surveys and studies

Figure 4: group of users and their motivational of using the social networks

It is clearly identified that the individuals group exposed to the potential privacy threats. In fact, the other groups can become the predator for the individual group to steal the personal information of the individuals.

Privacy is about something that we should keep secret from others. But keep something private in the public is madness and this is what happens to social networks services nowadays. For an example, Google is one of the main cloud storage for the Internet users. At the same time, it has Google+ for social network services. In here, the issue of privacy is critical as Google uses single sign-on method to access those services offered by them. It is easy whether you use the Gmail service, keep files in Google Drive, or upload photos to Google+, everything you write, upload, or post gets stored in a server that belongs to the online service, not to you. And because of outdated rules enumerated in the ECPA, this cloud-based data is vulnerable to a privacy loophole so big that a Google self-driving car could roll through it.

V. INFLUENCES OF SOCIAL NETWORK AND PERSONAL INFORMATION

The life of social network is on the users` personal information. Some of the social networks service member are willing to share their personal information to public and some are making private only for certain group. Amanda and Mary have conducted a survey and find out that for girls, social networking sites are primarily places to reinforce pre-existing friendships; for boys, the networks also provide opportunities for flirting and making new friends [17].

Each Internet user connected to social networks has a digital identity. It is made up of everything users publish on their various accounts and allows a sketch to be drawn of their personalities. The potential risk of the personal information on the social networks that the users might be facing are;

Stolen identity - this always happen someone has stolen somebody identity for certain purposes.

Pedophilia and sexual crimes - Teenagers, who are more numerous and more active on social networks, are exposed to sexual predators. Predators have time to make contact with their victims, most of the time under a false identity, and locate them geographically. The risk is even greater as teenagers are less likely than adults to be careful on these networks [16].

Illegal advertisement and spam - the online advertisement always refer to the user personal information. What they like, what they like to visit and many others on user’s personal information.

Government spy - the government might have been spying on each of the individual personal information. Snowden for example has revealed a leak saying that the government of United State is actually spying on each of individual citizen. This can be done via social networks.

Ideological manipulation - this scenario is considered to become the most crucial. People said Facebook can cause the fallen of a kingdom. Twitter can lead the change of the government faster. This is true when people are keep spreading their ideology regardless the information is correct or not.

VI. PRIVACY THREATS

We identify the following threats which will occur through social network;

New technology called "extreme-scale analytics" system created by Raytheon: according to US national government security, using Riot it is possible to gain an entire snapshot of a person's life – their friends, the places they visit charted on a map [18]. This new technology can track your movement all the time which is not acceptable by people. This is what we always ask how much privacy we still have not only on social network but also in our daily life. Photographs and videos that we post on social networks can easily lead to our location by using riots.

Facebook: in 2013 more people are quitting Facebook in concern with privacy according to new research. The reason why people do not use Facebook because they feel that they do not have enough privacy when using Facebook. When a user wants to leave Facebook there will be a display message asking the user why he or she wants to deactivated the account. However, photos and other information will be kept in Facebook the only thing that Facebook does when we deactivated the account is that photos and information will be hidden. This process has made people more concern about the privacy [19].

Porn Video Facebook Scam: we have seen such as these posts a lot appear on Facebook' wall from strangers. It is actually a crime and an invasion of privacy. By clicking on the link it will lead the user to a fake page which sometimes ask the user to like the page or install new software. Liking the page or installing new software is a malware. Once the users click on the link malware makes its way into a system, they begin to damage a system's boot sector, data [20].

Single access sign-on: using single access sing-on makes the user to access to several website easier but at the same time it is not secure as those websites will share information and other activities to other websites. Information should not be shared with other website, the user only can have the privilege but not the other. But yet social media share information as part of single access sing-on feature. As people are more concern on how to have more privacy when using single access sign-on, social media should improve the feature to ensure the level of privacy for the users [21].

Advertising harassment spam: in 2011 Facebook achieved advertising revenues of US $ 4 billion, according to its chief operating officer Sherly Standberg [22]. There are standards that companies must meet in order to use commercial advertising according to federal law and the Federal Trade Commission ("FTC"). According to FTC most of websites that use commercial advertising collected personally information from children. [23]

Personal information identity theft: personal information that we provide on social network is related to the third party of that specific website. When we talk about third party concept we keep in mind that weakness could happen in digital file of personal data and the information that kept in digital file possibly be revealed on the profiles of social network sites. One of the weakness is that when we sign in or search on the social network the information that we enter is attribute which are directly accessible by profile browsing. According to [24], social network users share a lot of information online, and SNS will record all interactions between users and keep them for potential use in social-data mining.

Phishing: personal information that we provide on social network can be easily found by the hacker if we do not protect the cookies. For instance, the email phishing attacks can be achieved 72% hit rate by using the information available in the social network [25]. Sensitive and important information are the targets for the attackers to attack, such as credit-card or bank account numbers and email passwords which can harm the user in case the hackers successfully get those information.

VII. RISK FACTORS ON SOCIAL NETWORK

As we discussed above, even though there is rare in terms of privacy on social network, there still have many people who tend to use this kind of services to be beneficial to them such as trading, teaching, news and so on. Therefore, this section we will discuss on risks factors which can lead the users in trouble. Thus users can use properly those services. To begin, there are several major factors that can reach users in privacy lose.

Firstly, lack of properly privacy setting. As we discuss above, privacy becomes a major concern in social network. It depends on users how privacy information do them willing to share to the rest of social network' users. Most of social networks allow users to set different privacy setting which user can decide to their private information to share or make it invisible [26] [27]. In contrast, majority of them are willing to skip the step of privacy settings by setting up as default.

Secondly, users have lots of trust in social network and their contacts [9]. They try to expose and shared whatever they want even if serious matters and try not to invisible sensitive information.

Thirdly, poor recognition in post. Users do not pay much attention on posting and information that they received. Whatever they got, they pretend to click and go forward even they do not what kind of information is?

Next, users always provide an e-mail which associated with their work to social network. This can lead to in terms of hacking when their e-mail is on anonymous person, it is easy to hack to their e-mail and gain information from it.

Furthermore, many users neglect to preview privacy policy and terms of services before signing up on social network.

In short, to be secure of using social network, at lease the user should aware and take consideration one of above factors.

VIII. PRIVACY DEFENSES AND AWARENESSES

As we discussed we have come out with some of the recommended strategies to prevent the threats as described below:

User should be aware about privacy and this can be done with self-awareness campaign: People and social network users specifically need to be more careful about the information they provide on their personal profiles in online social networks. Maintaining, reviewing and modification their information regularly is necessary to ensure the privacy.

Providing courses on social network security and encouraging awareness-raising: school and institute should intensively provide information on social network privacy as most of students now use social network in daily life. As well as to inform the users to make the rational usage of the Social Networking Sites to develop and practice security concern and policies.

Using stronger authentication and access-control: having a strong password can protect personal information but yet there will be risks. The strength of authentication is different from site to another site, in order to provide strong defense we need to use additional authentication factors such as e-mail verification through Captchas as well to use spam filter.

IX. CONCLUSION

Technology and social network have made interaction and communication much easier than early decade. In this paper, we have briefly come across privacy on social network. As many websites and social networks out there, people are more concern on how much privacy do they still have. We have also highlighted what is the current situation on using social network, as well as what are the threats that can affect the users on social network activates as almost everything we post or share on website will be shared with others. Finally, we have stated some security and privacy awareness that can be practiced in order to be more aware of social network threats.

REFERENCES

[1] Blackboxsocialmedia, "blackboxsocialmedia," [Online]. Available: http://blackboxsocialmedia.com/social-networking/. [Accessed 25 December 2014].

[2] L. A. Cutillo and R. Molva, "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust," *IEEE,* pp. 94-101, 2009.

[3] A. Srivastava and G. Geethakumari, "A Framework to Customize Privacy Settings of Online Social Network Users," *IEEE Recent Advances in Intelligent Computational Systems (RAICS),* pp. 187-192, 2013.

[4] A. Srivastava and G. Geethakumari, "Measuring Privacy Leaks in Online Social Networks," *International Conference on Advances in Computing, Communications and Informatics (ICACCI),* pp. 2095-2100, 2013.

[5] A. Dhami, N. Agarwal, T. K. Chakraborty, B. P. Singh and J. Minj, "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook," *3rd IEEE International Advance Computing Conference (IACC),* pp. 465-469, 2013.

[6] B2BInternationalInConjunction and KasperskyLab, "CONSUMER SECURITY RISKS SURVEY 2014: MULTI-DEVICE THREATS IN A MULTI-DEVICE WORLD," Kaspersky Lab, 2014.

[7] W. Binden, M. Jormae, Z. Zain and J. Ibrahim, "Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks," *International Journal of Scientific and Research Publications,* vol. 4, no. 1, pp. 1-6, 2014.

[8] X. Chen and S. Shi, "A Literature Review of Privacy Research on Social Network Sites," *International Conference on Multimedia Information Networking and Security,* pp. 93-97, 2009.

[9] F. Raji, A. Miri and M. D. Jazi, "Preserving Privacy in Online Social Networks," *Springer-Verlag Berlin Heidelberg 2012,* pp. 1-13, 2012.

[10] J. Ge, J. Peng and Z. Chen, "Your Privacy Information are Leaking When You Surfing on the Social Networks: A Survey of the degree of online self-disclosure (DOSD)," *IEEE 13th Int'l Conf. on Cognitive Informatics & Cognitive Computing (ICCI*CC'14),* pp. 329-336, 2014.

[11] Statista, "Statista," October 2014. [Online]. Available: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. [Accessed 25 October 2014].

[12] "GO-Gulf," GO Gulf Web Design Dubai Company, 14 July 2014. [Online]. Available: http://www.go-gulf.ae/blog/what-people-share-on-social-networks/. [Accessed 31 October 2014].

[13] "Social Networks: Global Sites Ranked by Users 2014 | Statistic." *Statista*. Web. 7 Nov. 2014.

[14] Lucas, Matthew M., and Nikita Borisov. "Flybynight: mitigating the privacy risks of social networking." *Proceedings of the 7th ACM workshop on Privacy in the electronic society*. ACM, 2008.

[15] Dwyer, Catherine, Starr Hiltz, and Katia Passerini. "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace." *AMCIS 2007 Proceedings* (2007): 339.

[16] Guy-Hermann Ngambeket Ndiandukue." Social Networks and Privacy—Threats and Protection ." *Isaca Journal, Volume* 5, 2012.

[17] Lenhart, Amanda, and Mary Madden. *Social networking websites and teens: An overview*. Pew/Internet, 2007.

[18] R. Gallagher, "Software that tracks people on social media created by defence firm," 3 February 2013. [Online]. Available: http://www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence. [Accessed 3 November 2014].

[19] V. Woollaston, "Mail Online," 17 September 2013. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2423713/Facebook-users-committing-virtual-identity-suicide-quitting-site-droves-privacy-addiction-fears.html. [Accessed 3 November 2014].

[20] "Trend micro," [Online]. Available: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/9-social-media-threats-you-need-to-be-aware-of. [Accessed 3 November 2014].

[21] "reputaion.com," [Online]. Available: http://www.reputation.com/reputationwatch/articles/top-five-social-media-privacy-concerns. [Accessed 3 November 2014].

[22] G.-H. N. Ndiandukue, "Social Networks and Privacy—Threats and Protection," *ISACA,* vol. 5, pp. 19-23, 2012.

[23] "Privacy trust," [Online]. Available: http://www.privacytrust.org/guidance/commercial_privacy.html. [Accessed 28 October 2014].

[24] A. Al hasi, "Threats of online social network," *Seminar on internetworking,* 2008.

[25] A. Al hasib, "Threats of online social network," *Seminar internetworking,* 2008.

[26] P. Nguyen, "Hotspotshield," 25 June 2013. [Online]. Available: http://blog.hotspotshield.com/2013/06/25/social-media-privacy-concerns/. [Accessed 17 November 2014].

[27] C. Wüest, "The Risks of Social Networking," Symantec Corporation, 2010.

AUTHORS

First Author – MafaisuChewae, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and Faa.izoon@gmail.com.
Second Author – SameerHayikader, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and sameer797.kader@gmail.com.
Third Author – MohammadKhairulNizam, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and redspira@gmail.com.
Fourth Author – Jamaludin Ibrahim, Adjunct Lecturer and Senior Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and jamal55@gmail.com.