ISSN 2250-3153

# Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks

**WorawitBinden*, MaheedeenJormae**, ZakariaZain***, Jamaludin Ibrahim******

worawit.inter@gmail.com*, maheedeen@gmail.com**, zakariazain13@gmail.com***, jamal55@gmail.com******

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

***ABSTRACT***-Use of Online Social Networking Sites (OSNs) has become ubiquitous nowadays. In the era of a million user social networking sites throughout the world, it becomes increasingly difficult for people to control what they are exposing to whom. In this paper we analyze the influence of social media interactivity features on the exposure of personal data of average Internet user and present techniques to implement information security awareness to minimize over-exposure on OSNs.

***Index Terms***-Online Social Networking, Information Security Awareness, Social Network Interactivity Features

## I. INTRODUCTION

Information is vital to communication and a critical resource for performing work in organizations. It is also important to individuals, and therefore the need to proper manage it well, is growing rapidly. Protecting data is as important as protecting cash as it is asset – and requires just as much care and planning. Now more than ever, people need to understand the critical role information plays in so many aspects of business and life. It drives our communication, our decision-making, and our reactions to the entire environment.

Information has been valuable since the dawn of mankind. As access to computer stored data has increased, Information Security has become correspondingly important. In the past, most corporate assets were "hard" or physical: factories, buildings, land, raw materials, etc. Today far more assets are computer-stored information such as customer lists, proprietary formulas, marketing and sales information, and financial data. Some financial assets only exist as bits stored in various computers. Many businesses are solely based on information – the data IS the business.

Information Security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved confidentiality, possession (or control), integrity, authenticity, availability and utility [17]. Sensitive information must be kept - it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat.

Information Systems (IS) have a variety of important functions, ranging from allowing businesses to keep track of customers, products, and trends, to public health organizations keeping. Therefore, information systems are crucial assets as they improve the efficiency of operations in order to achieve higher profitability and competitive advantages to the same industry competitors. They also aid in the creation of new products and services as well as improvement of the decision making process. Information systems are additionally considered an integral part of today's business [13]. All the vast data that is communicated on electronic devices is stored into these systems. Multinational organizations are globally distributed. They require a reliable infrastructure, which can handle processing requirements.

In the era of high Internet penetration, social networking sites, while not an entirely novel phenomenon, have become increasingly more popular in recent years. Networking sites such as Facebook, Twitter and Google+ have become a significant part for most of people around the globe. Facebook alone is accessed by over 23 million users [18]. There is a tension between the lucrative business side of social networking sites, where huge monetary gains can be made through online advertising, and the companies' resolve to ensure a basic level of privacy for its users. From this tension users receive privacy setting recommendations from social networking sites whose default settings are rarely altered or even questioned. The privacy problems that ensue stem from the fact that individuals are unaware of the amount of personally identifiable information they have provided to an indeterminate number of people.

As the world of social networking become more popular, Facebook increased the availability of its product, opening doors to new networks and members. What began with restricted access to students with valid university-issued e-mail addresses, spread to allow high school and corporate networks as well as users without verified e-mail addresses. These users can create profiles, and gain access to information on other members of the site (Social networking on the Internet began with a desire for people to quickly and conveniently share information with their friends and family. This form of communication blossomed rapidly and started competing in popularity with e-mail and text messaging. Entrepreneurs harnessed this technology and created various Internet sites, including Facebook and MySpace, designed to allow users to create a profile containing information about themselves that others can view. These sites also allow users to build social networks with hundreds or even thousands of people. Previously, the use of these websites posed little known threat to personal privacy and users' comfort levels changed.

The purpose of information security awareness is to enhance security by improving awareness to protect information.

In this online era, information security awareness provides the understanding of security policies to the Internet users to guide them in protecting their information assets.

The researchers in information security argued that most of the Internet users are unaware that their habits in using computer can adversely impact the security and privacy of their own personal data [15]. According to Johansson and Riley (2005) [16], "Helping people to understand their own security vulnerabilities and how to, well, 'patch' them is the most effective way we know of to help educate people about computer vulnerabilities and to protect personal information".

In short, the Internet users have to be aware of their vulnerabilities in order to protect their assets.

## II. LITERATURE REVIEW

### *A.Information Leakage onOnline Social Networks*

In the era of Internet technology, online social networks (OSNs) becomes a wide-ranging used over the world, more and more third-party enterprises take this opportunity to exploit data from OSN websites, which have been collected from social media users [16]. The information that is available in the users' profile can be searched based upon different criteria and thus can also be accessed by the strangers. Most of the people tend to expose real identity information; so that it raises privacy and security issues [11]. Nonetheless, there are a large number of OSN's users who are not aware of the personal data revelation, as their information tends to bring to public. Consequently, Feizy (2007) founds that social media users reveal their information widely on their pages. Although a large number of them expose that appears to be real identity information. He also demonstrates the overall network of participants' identity exposure as we can see from the figure 1 below. As the quality and quantity of information illustrated by different size and patterns whereby a large set of identity combination was collected to find some relation in peoples' behavior [10].

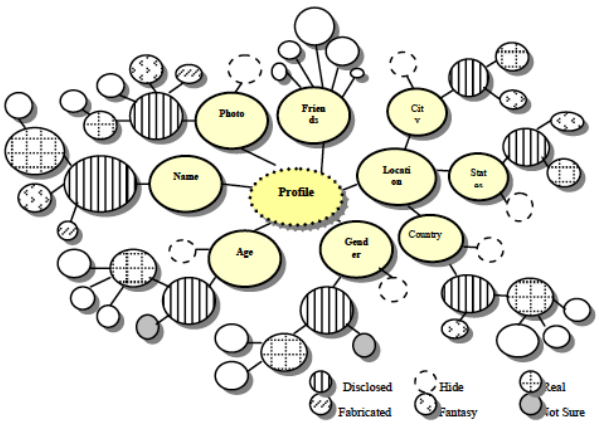


Figure 1: An Overview of Personal Information Disclosure [10]

According to Koehorst (2013), people have to reveal personal information such as name, date of birth and contacts in their OSN-profiles in order to be effective, and adolescents just have to do this to sound out their maturing identities". In fact, communication on the Internet can lead to more disclosure compared to face-to-face communication and the other ways. Despite that the personal information-related behavior of people can be conceptualized as a continuum. This continuum can be described as "information privacy protection behaviors such as information withholding and incomplete and inaccurate disclosure on one side, and complete and accurate information disclosure behaviors on the other." On OSNs this means that users can still participate all whilst attempting to protect their personal information by only partly disclosing personal information [4].

### *B.Information Security and Online Social Networks*

Since information can be leaked through OSN, face-to-face conversation and printing facilities, email, cloud computing, domain name systems and portable data devices. This is because information disclosed through OSNs creates an opportunity for cybercriminals to do surveillance and gather intelligence, sabotage organizations' networks using malware and utilize resources to launch attacks through the applications on these sites [2]. They also describe the typical functionalities of OSN sites, which are being implemented in many social media websites such as Facebook, Google+, and Twitter in order to make potential avenues of information disclosure. The table below represents OSN's capabilities as attack vectors through its available functionalities.

Table I: OSN Function and Potential Problems to Organization [2]

| OSN Functionalities | Potential Security Problems | Impacts to Organisations |
|---|---|---|
| Post information / update status | Accessibility of OSN by anyone, anywhere at anytime, using any devices, allows users to update their status several times a day, thus, sensitive information may be revealed. | Revealed information can be deduced by attackers to obtain confidential information about the organisations in order to do cyber espionage and sabotage. |
| Friends' Requests | Carelessness in accepting friends' requests could result to adding 'enemies' instead of 'friends' who have more access to users' information. | These 'friends' are able to constantly monitor the employees' activities within the organisations allowing them to obtain employees' credentials for accessing the corporate network. |
| Upload photos and videos | Unrestricted photo albums and videos allow everyone to view the photos and videos that are potentially sensitive to organisations. | Sensitive photos and videos may cause embarrassment to the organisations and they may be useful for cybercriminals to collect information. |
| Third party applications and links to external sites | While using the applications or clicking on the links, malware may infect employees' computing platforms. | Compromised client platforms allow attackers to sabotage corporate networks and provide access to monitor and steal intellectual property. |

Furthermore, throughout the users' information revelation, someone else can easily disclose the personal data because the users' friends can post or publish their information to other friends. Likewise, the users' information can be commonly shared or sold to marketing company for advertising practice and selling product. Recently, it has been found that there are various of social media users have been attacked by spams, phishing, and malware through OSN applications by clicking on the advertising application as some of advertisements may contain a malicious tracking to steal personal data or attack users' devices.

Additionally, security awareness on OSNs has to be very concerned among Internet users in order to avoid from malicious cyber activity. There are some of key points that recommended in any awareness program concerning social media sites[14].

1) *Privacy & Social Media***:** Privacy does not exist on OSNs. Although, many social medias like Facebook, Google+, and Twitter provide privacy options and controls, but too much can go wrong and our sensitive information can end up being exposed such as our account being hacked, our friends' account being hacked. This means that being careful and watching what our friends post about us, including pictures. If nothing else, remember that employers now include sites like Facebook, Google+, and Twitter as part of any standard background check [14].

2) *Scams & Social Media:*OSNs are a breeding ground for scams. If one of our friend's posts seems odd or suspicious, it may be an attack. For example, our friend posts that they have been mugged while on vacation in London and need us to wire them money. Or perhaps they are posting links about great ways to get rich, or some shocking incident we must see. Many of these scams or malicious links are the very same attacks that we have been receiving in e-mail for years, but now bad guys are replicating them in social media. If we see a friend posting very odd things, call or text them to verify that they really posted the information [14].
3) *Work & Social Media:* Working information is not recommended to be revealed on OSNs, therefore, it is better not to post anything sensitive about work such as company name, company address, or colleges' profile. Also, be sure that we understand about organization's policies as what we can and cannot post about job information [14].

### *C.Recent Online Social Networks Activities Statistics*

Today, the number of online social networks users like Facebook, Google+, and Twitter is growing rapidly, there are still many people who are not concerned on privacy settings as they do not realize that the information that are being publicly shared will be exploited by anonymous person.

| | 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: Recent Statistics of Social Medias Activities in Q2, 2013 [7]

Regarding the recent statistic of online social media networks usage, which has been found in the second quarter of 2013 described that.

Firstly, more than 800 million of active users in Facebook uploaded and shared photos, which is dominated among Google+ and Twitter in nowadays, about 580 million clicked Facebook 'like' button, and almost 287 million of the users posted comment about my daily activities. Approximate 469 million of users followed a group or like a page created by a brand [7]. In contrast, there is only 25 percent of Facebook users do not pay much attention on privacy settings [8].

Secondly, Google+ has about 370.48 million of active users uploaded and share photos. Performing an activity on Google+ '+1' button clicked, which is nearly 233 million of users and posted comment about my daily activities is over 260.43 million of users [7]. Recently, following a group or like a page created by a brand activity is not yet found in Google+.

Last but not least, there are about 323.22 million of Twitter users uploaded and shared photos on Twitter website, over 280 million of users posted comment about my daily activities. Twitter users followed a group or like a page created by a brand, which has about 191 million of users [7]. On the other hand, clicking 'like' activity in Twitter was not found, as Twitter does not provide this feature.

### *D.Privacy Concerns with OSNs Service*

Privacy is a multifaceted concept, and this results in a multitude of definitions and concepts. A widely accepted view of privacy is "the individual's right to be left alone." There has not been a consensus about the definition of privacy, stating that "perspective on privacy are thus varied, occasionally conflicting, and generally difficult to evaluate in a coherent fashion" [4]. In other word, privacy implications associated with online social networking depend on the level of identifiability of the information provided, its possible recipients, and its possible uses [5].

Social media companies like Facebook,Google, and Twitter generally have their own privacy policies that govern their use of consumer data and third-party conduct on the social media platform with respect to personal data [23]. In order to utilize third-party social media outlets, Steinman & Hawkins (2010) suggest that marketers need to ensure on their marketing campaigns, which will not persuade consumers or any other parties to engage practices that would violate the social media company's privacy policy, and marketers also need to ensure that they are abiding by the policies. Additionally, the description below represents the comparison of privacy setting in online social networks e.g., Facebook, Google+, and Twitter [23].

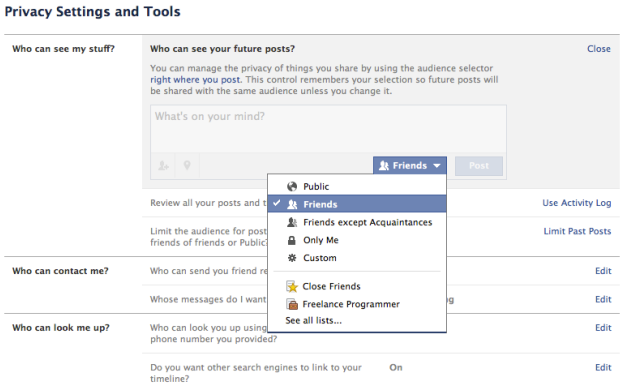


Figure 3: Privacy Settings in Facebook

Facebook: Its privacy options are generally very flexible because users can select from when they post something to their profile: "Public" and "Friends." As its name suggests, the "Public" option means that items they publish to their profile are visible to anyone who visits Facebook. Similarly, selecting "Friends" allows only their Facebook friends to see what they post. Furthermore, Facebook also offers a "Custom" setting as users can choose who gets to see that they post by either restricting it to any networks they are part of or so that only people only selected "lists" (a way to organize their friends

into groups). In addition, users can also prevent specific people from seeing items they post [6].

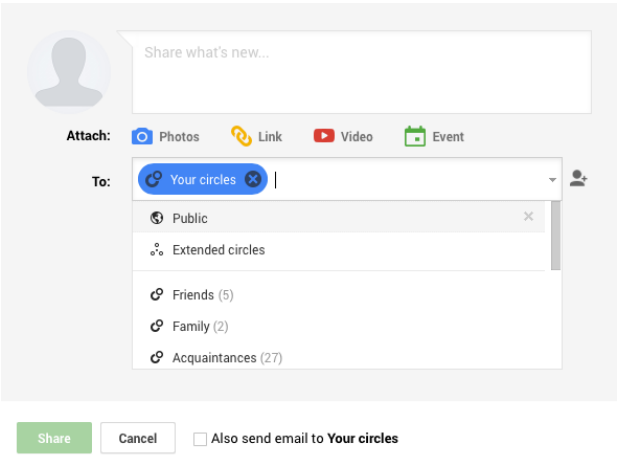


Figure 4: Privacy Settings in Google+

Google+: Its privacy is built around the concept of "Circles", which is similar to lists on Facebook, Circles let users organize people they follow on Google+ into groups based on how they know them. For instance, users may have one Circle for friends, one for family members, one for close confidants, and one for coworkers. When users post something to Google+, they can specify which of their Circles they want to share that particular post with. Alternatively, they can make something public so that anyone can see it, pick and choose which individual Google+ other users can see their posts, or choose to share it with [6].

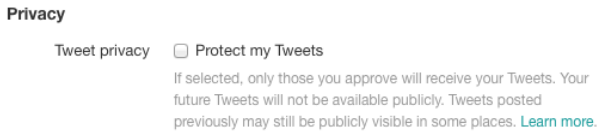


Figure 5: Privacy Setting in Twitter

Twitter: Its privacy settings are quite basic, but then again, the social network is conceptually much simpler than both Facebook and Google+. Twitter profiles can be either private or public, and users can swap back and forth between the two as they please. Selecting "Protect my Tweets." to change account into private account. When users' account is private, only those they approve can see their tweets, and their tweets cannot be retweeted. Users' bio, name, and Twitter handle are always visible, though [6].

In addition, there are many of the popular OSNs, which have released web APIs to allow third-party developers and websites to implement their own services that can utilize and aggregate user information and activities in OSNs [9]. As Facebook, Google+, and Twitter provide these particular social network platforms to integrate with third-party applications in order to access cross the users' profile. In spite of that users have to be careful on permission granted before allow them getting into their personal information so that their information will be disclosed by anonymous third-party applications.


Figure 6: Example of Request for Permission in Facebook Apps

In order to be aware of using third-party applications, users must be ensured that those applications that are requesting for permission is mostly well known among people in online social networks. This is one of the basic practices in data protection to avoid of personal information leakage to stranger.

## III. THE INFLUENCE OF OSNS' INTERACTIVITY FEATURES

Based on the static from December 2012 to May 2013 [12], Facebook is the most significant online social network that people often visit monthly while Twitter and Google+ have less amount of usage respectively. In this paper, we are going to compare the most interactivity features of OSNs that can lead to over-exposure of personal data of average Internet user

Table II: OSNs' Interactivity Features Comparison

| Facebook | Twitter | Google+ |
|---|---|---|
| 1. Facebook structure<br>• News Feed<br>• Friend<br>• Wall<br>• Timeline<br>• Like<br>• Messages and inbox<br>• Notifications<br>• Networks, groups, and pages<br>**2. Applications**<br>• Events<br>• Marketplace<br>• Notes<br>• Places<br>• Platform<br>• Questions<br>• Photos<br>• Videos<br>**3. General features**<br>• Credits<br>• Feature phones<br>• Graph Search<br>• IPv6<br>• Listen with Friends<br>• Facebook Live<br>• Mood faces<br>• Phone<br>• Poke<br>• Smartphone integration<br>• Subscribe<br>• Ticker<br>• URL shortener<br>• Verified Accounts<br>• Hash tagging Feature<br>**4. Languages**<br>**5. Security** | **1. Main Features**<br>• Following/Follower<br>• Tweet/Retweet<br>• Direct Messages<br>• Photo Uploading<br>**2. Additional Features**<br>• Location Service<br>• Hashtaging<br>• Trending Topics | **1. Main Features**<br>• Stream<br>• Circles<br>• Hangouts<br>• People<br>• Photo<br>**2. Additional Features**<br>• Messenger<br>• Instant Upload<br>• Spards<br>• Games<br>• +1 button<br>• Hashtags<br>• Ripples<br>• Google+ Badges<br>• Google+ Local<br>• Google+ Events<br>• Google+ Communities |

To sum up, the above table shows that Facebook offers more interactivity features, which lead to over-exposure than others. So Facebook users expose their personal data every second to public.

## IV. PROPOSED FRAMEWORK

In order to minimize the over-exposure of Internet user on OSNs, this proposed framework could be suggested as one of the existing frameworks to avoid users revealingtheir personal information in public.From the framework below we can see thatOSNs offer many interactivity features to convince their users to reveal their personal information voluntarily. So we

believe that by employing IS awareness among the OSNs users can minimize the over-exposure of their personal information.

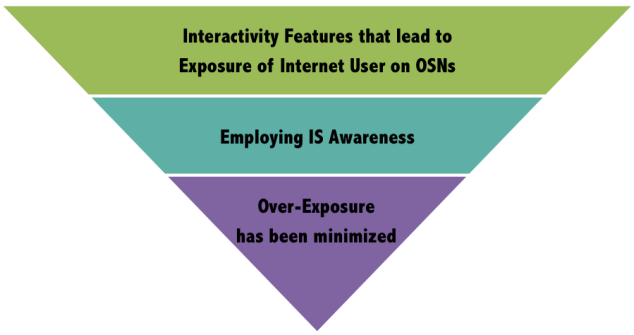


Figure 7The Proposed Framework to Minimize Over-Exposure

Unfortunately, there is no any beneficial information security tool that can effectively reduce over-exposure of social media users in nowadays. It is only awareness of using OSNs, which can be best suggested. Since, OSNs generally provide users with a profile section, facilitate for uploading and sharing contents such as photos, music, etc., and messaging in various forms on the wall, and also enabling to put comment on friends' posts. All in all, OSN is quite new platform of interacting online where users in a virtual network are able to share information and communication with one another.

In regard with the finding that has been found in two separated studies mentioned that 79 percent of social media users do not much concern on changing of the default settings as can be obviously seen in Twitter, whereby about 99 percent of users preferred default its settings, this study was conducted by Mannan. Yet, only 1.2 percent indicated that the percentage of users who changed the default privacy setting is very small number, this was found in Gross's study [19]. Moreover, another study had been conducted in 2009 represented that there are 51% of students, 44% of employees, and 5% of the other from 144 participants. It is summarized that 76% of those participants do not notice about the risk of representing some of their information online warned by OSN providers. There is nearly 45% of students show that users are not given any list or guideline by OSN providers regarding this issue [20].

According to the study ofHasan and Hussin (2010), which has proposed awareness to minimize those activities on OSNs that could be about privacy, information security in line with the users' educational, moral, and ethical values while they are in OSNs[20].

1) *Awareness during sign-up in OSNs:*There are many of OSNs do not make availability of information for prospective social media users on which information to enter in any fields for user registration. Moreover, users do not have sufficient concession to customize their profile information and do not obtain any guidelines during pre-registration on the OSN site. Hence, it is required for a new user in being aware of which information needs to enter into the systems provided by OSN sites [20].
2) *Being aware of things, while writing on OSNs:* Regarding the study, which was conducted in 2009, out of 144 of participants had given opinion that the following kind of information in OSNs should be strictly concealed in public as represent in percentage such as passwords (92%), national identity card number or security number as personal identification information (83%), religious beliefs and political opinions (31%), e-mail address (29%), location-related information (26%) or personal pictures (13%) [21].
3) *Setting appropriate defaults of privacy preference:*Furthermore, according to the study of Hasib (2008) recommended that more and more social media users are lessin paying attention on essential for setting the default privacy preference in OSNs [22]. Therefore, it is necessary to change the default privacy setting as secure as possible in order to avoid personal information leaked while using OSN sites [11].
4) *Building self-awareness about the information disclosure:*Hasib (2008) also emphasized that social media users have to be more concerned about their information, which are represented through personal profiles in OSNs. Also, those particular personal profile contents have to be precisely maintained to secure proper revelation of information in OSNs [11].

## V. CONCLUSION

In the nutshells, information security awareness is very important to be applied in everybody's life in order to minimize the over-exposure of their personal information in online social networking, especially Facebook, Twitter and Google+. OSNs user should be fully aware about their personal details and their information are not easy to give and expose to the public. We believe that employing IS awareness among OSNs will minimize over exposure, even though OSNs provide variety of interactivity features to convince user to voluntarily expose their personal information.

## REFERENCES

[1] Li, N., N. Z., & Das, S. K. (2011, MAY/JUNE). Preserving Relation Privacy in Online Social Network Data. *Security & Privacy in Social Networks* , 35-42.
[2] Abdul Molok, N., Chang, S., & Ahmad, A. (2010, November). Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. *Proceedings of the 8th Australian Information Security Mananagement Conference* , 70-80.
[3] Alim, S., Neagu, D., & Ridley, M. (2012). A vulnerability evaluation framework for online social network profiles: axioms and propositions. *Int. J. Internet Technology and Secured Transactions, 4*, 198-206.
[4] Koehorst, R. H. (2013). *Personal Information Disclosure on Online Social Networks.* University of Twente, Department of Communication Science, Enschede.
[5] Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Network (The Facebook case). *ACM Workshop on Privacy in the Electronic Society (WPES)* .
[6] Mediati, N. (2012, Jun 29). *Social network privacy setting compared*. Retrieved Oct 28, 2013, from TechHive: http://www.techhive.com/article/2000181/social-network-privacy-settings-compared.html
[7] Bullas, J. (2013, Sep 19). *12 Awesome Social Media Facts and Statistics for 2013*. Retrieved Oct 29, 2013, from Business 2 Community: http://www.business2community.com/social-media/12-awesome-social-media-facts-statistics-2013-0622265
[8] McGrall, M. (2013, Oct 1). *Infographic - Social Media Statistics for 2013*. Retrieved Oct 27, 2013, from Velocity Digital Blog: http://www.velocitydigital.co.uk/infographic-social-media-statistics-for-2013/
[9] Cheng, Y., Park, J., & Sandhu, R. (2013). Preserving User Privacy from Third-party Applicaiton in Online Social Networks. *The International World Wide Web Conference Committee (IW3C2)* , 723-728.
[10] Feizy, R. (2007). An Evaluation of Identity on Online Social Networking: Myspace.
[11] Al Hasib, A. (2008). Threats of Online Social Networks. *Seminar on Internetworking* .
[12] Ray, A. (2013, Jul 23). *The Real Data on Facebook vs. Google+ (And Other Social Networks) [INFOGRAPHIC]*. Retrieved Nov 4, 2013, from Social Media Today:

http://socialmediatoday.com/augieray1/1613711/real-data-facebook-vs-google-and-other-social-networks-interactive-infographic
[13] Wikipedia. (2013, Oct 31). *Information Systems*. Retrieved Nov 9, 2013, from Wikipedia.com: http://en.wikipedia.org/wiki/Information_systems
[14] Ispitzner. (2012, Oct 1). *Security Awareness on Social Media*. Retrieved Nov 8, 2013, from Educause: http://www.educause.edu/blogs/lspitzner/security-awareness-social-media
[15] Anderson, C. (2005). Creating Conscientious Cybercitizen: An Examination of Home Computer User Attitudes and Intentions Towards Security. *Paper presented at the Information Systems* .
[16] Johansson, M. J., & Riley, S. (2005). Protect your wisdom network-from perimeter to data. *Addison Wesley Professional* .
[17] CENGAGE Learning. (2013). *CENGAGE Learning.* Retrieved Nov 8, 2013, from Introduction to Information Security: http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf
[18] Facebook. (2007, Apr 11). *Facebook.com.* Retrieved Nov 8, 2013, from FAcebook Overview: http://harvard.facebook.com/press.php
[19] Schrammel, J., Koffel, C., & Tscheligi, M. (2009). Personality traits, usage patterns and information disclosure in online communities. *23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* , 169-174.
[20] Hasan, M. R., & Hussin, H. (2010). Self Awareness before Social Networking: Exploring the User Behaviour and Information Security Vulnerability in Malaysia. *Proceeding 3rd International Conference on ICT4M* , 7-12.
[21] Aimeur, E., Gambs, S., & Ho, A. (2009). UPP: User Privacy Policy for Socail Networking Sites. *Proceedings of the Fourth International Conference on Internet and Web Applications and Services* , 267-272.
[22] Mackay, W. (1991). Triggers and barriers to customizing software. *Proceedings of CHI'91* , 153-160.
[23] Steinman, M. L., & Hawkins, M. (2010, May). When Marketing Through Social Media, Legal Risks Can Go Viral. *VENABLE LLP ON ONLINE MARKETING LAW* .

## AUTHORS

**First Author** – WorawitBinden, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and worawit.inter@gmail.com.
**Second Author** – MaheedeenJormae, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia andmaheedeen@gmail.com.
**Third Author** – ZakariaZain, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and zakariazain13@gmail.com.
**Fourth Author** – Jamaludin Ibrahim, Adjunct Lecturer, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and jamal55@gmail.com.