

## Facebook Proliferation in Contemporary Youth Society Vis-à-vis the Privacy Management and User Perceived Behavior Control

Norulhuda Tajuddin<sup>1\*</sup>, Mohamad Ridhuan Mat Dangi<sup>2</sup>, Norizzati Binti Bahsri<sup>3</sup>,  
Zarirah Zamakhsari<sup>4</sup>

<sup>1,3,4</sup>Faculty of Business Management, Universiti Teknologi MARA Pahang,  
26400 Bandar Tun Razak Jengka, Pahang, Malaysia

alhudatajuddin583@pahang.uitm.edu.my, izzatibahsri@pahang.uitm.edu.my, Zarira2939@pahang.uitm.edu.my

<sup>2</sup>Faculty of Accountancy, Universiti Teknologi MARA Selangor  
40450 UiTM Shah Alam, Selangor, Malaysia

ridhuan@salam.uitm.edu.my

\*Corresponding Author

**Abstract:** Technological advancement nowadays not only comes out with sophisticated and cutting edge products, but it also has change the way human communicates with each other's. The adoption of internet technology in communication has developed a new dimension of virtual world where people can communicates and interacts online using various social networking media as the channel. To date, Facebook is one of the most popular social networking media with millions of users around the globe. It allows people to interact and connect with others crossing the regions, creates profile and sharing information, uploads photos and videos, send message and keep in touch with friends and so on. Teenagers and young adults are the major users of this social networking media. Despite the benefits and versatility, most people are not aware and take for granted about the privacy concern while using Facebook. Sometimes what is posted on Facebook contain many personal information that could be misused by criminals and unscrupulous individuals that targeted the victims. Therefore, Facebook users must be aware and should wisely use this social networking media and avoid themselves from becoming victims to cybercrime. Hence, this paper attempts to investigate the privacy management among the Facebook users. Further, the researchers also tries to examine how the users control themselves when using the Facebook features such as exchange information, sharing photos, comments and so forth. On top of that, this paper will assess the user's behavior and their concern about the privacy management and other security settings in Facebook.

**Keywords:** Facebook, Privacy management, Social networking media, Threats

### 1. Introduction

The rapid advancement of technology has changed the world. The transition from each phase of centuries has shown many remarkable innovations and the growth of technology from basic in nature until the sophisticated and futuristic products. This includes the new communication media and the rise of smartphone and other mobile devices. According to Chen (2012) cited in Wooley (2013), this new media has revolutionize the human and society interaction to a highly interconnected and complex level. The internet also associated with the advancement of technology that allows computers and other devices interconnected to each other's in a global system. The adoption of internet as a medium for communication has transformed the world in the way to communicate and interact with each other's. Under this means, the new communication media combine with the technological advancement allows people around the world to communicate instantly along with interactive online experience. Not only it can alleviate the communication process, but it also offers many interesting features and attractive characteristics for the users.

In this information age, the social networking media has become a mainstream activity and major technological phenomena with hundreds of millions of people participating around the world. (Squicciarini et al., 2009). There are various social networking media such as

Myspace, Friendster, Twitter, Line, WhatsApp, Instagram and the most popular today is Facebook were used as a channel for the people around the world communicating with each other's. Since it is free to join with only requires a valid e-mail address and aged above 13 years old, everyone can enjoy using these social networking media for numerous purpose and activities. Among others, it allows people to exchange information, sharing photos and videos, business activities and so forth. In fact, the major users for the social networking media are teenagers and young adults as well as the university students (Borneo and Barkhuus, 2011). In this paper, it emphasizes on the use of Facebook and how the users manage their privacy concern in using this social networking media.

Facebook is co-founded by Mark Zuckerberg with his college roommates and fellow Harvard University students in the year 2004 initially to serves as a way for the college and university students to keep in touch when they had left campus (Croft, 2007). At present, Facebook has evolved and become the largest social networking website in the world and worth billions of dollars of investments. Available with 37 different languages, Facebook also have public or basic features such as 'marketplace', 'groups', 'events', 'pages', and 'presence technology'. While other networking components featured in Facebook are the 'wall', 'photo album', 'status updates', 'microblogging', 'newsfeed' and other numerous components for its users. Other than that, it also offers users a range of privacy options. The users can choose whether the communications will be visible to anyone, blocks the specific connections or make the communications in private. Users also can choose whether they wanted to be searchable or not, determine which part of the profiles to be public, decide the party who can see the posts and so on. In other words, it depends on the users to set up their privacy settings as they wanted.

The issues of privacy concern in online and social networking media receive a significant attention from various researchers (Gummadi, 2013). This is because some of the information shared during the online activities using the social networking media could draw negative impact and any unwanted events. The information posted on Facebook especially that related with the personal information such as address, phone number, pictures, account numbers are sufficient enough to open potential threats for the users when dishonest individuals tend to misuse the information for criminal activities. For example, in certain cases, some of the criminals are spreading the computer viruses, malware and even spam message through the link of fake web address (Sophos Inc. 2013). Meanwhile Al Hasib (2008) categorized the potential threats of using social networking media into four groups. The first is privacy related threats where the information revealed in the social media will be exploited to embarrass, blackmail, or damage the reputation of the users. Second are the social networking media variances of traditional network and information security threats has encourage the spammers to cause the traffic overload, loss of trust or difficulty in using the underlying application as well as phishing and diversion to pornographic sites. Next is the identity related threats which is the risk of criminal action performed through the hacking of sensitive information such as passwords, credit card and bank account numbers that will cause financial and reputation damage. The fourth is social threats that will happen when the information such as location, phone number, address etc. in the user's profile were used by the criminals such as cyber stalking that potentially can cause a physical harm and psychological damage to the victims.

The problems for privacy concerns also emerged when various social networking media including the Facebook launches the social networking platforms that allows third party developers to contribute the applications and widgets as some additional functions (Cheng et al., 2013). Although they have a legal rights since both of the social networking media and the third party developers have a commercial benefits, however the users still facing the risks when their personal information are exposed to violation. Other than that Facebook users also will receive lots of information from their online activities using this social media. The worrying part is not all of the information is true or inclusive (Robert Lee, n.d.). People can suffer from information overload because if such information were absorbed blindly, it potentially tempt the users to become the victims of cyber related crimes such as hacked personal information, cheating, blackmail, and other threats. The key to use these social networking media in safe conditions

required users to wisely manage and control their privacy and personal information when they are online. Thus, how far the user realizes and aware about the privacy statement when using the Facebook or other social networking media has become the concern and the catalyst to drive the researchers to convey in this study.

## 2. Literature Review

Since its inception in 2004, Facebook has grown rapidly and gains popularity as it is seen nowadays. As one of the renowned social network sites which attracted millions of users around the world, Facebook allows its users to create profiles, upload photos and videos, send messages and keep in touch with families, friends and other users. The immense and growing popularity of Facebook catch the attention not only for the users to use it but also draw the interest for a fascinating field of study. As such, the privacy matters are among of the rising researchers concerns when using the internet especially the social networking sites. Digital privacy has been a consistent concern since the Internet became a popular medium in the 1990s (Marwick et al., 2010). Indeed, the Facebook and other social networking sites have provided the privacy settings for all its users. Privacy settings are useful to those who are sharing information so that they can manage who gets access to that information (Boyd and Hargittai, 2010). However, it is still speculative whether the privacy settings provided by this social networking sites really securing the user's privacy. Somehow, the users itself are not concern with their privacy information when using the internet. This is found by Debatin et al. (2009) in their studies found that many Facebook users are not changing default privacy settings, making them rely on lax, initial startup settings.

Some of us might not realise that the internet is not completely private and it is difficult to avoid from the mischief activities such as stealing identity, abuse of information and other related risks that could harm users. The Facebook itself capable to store an immense amount of the user's personal information, including name; birthday; political and religious views; online and offline contact information; sex, sexual preference and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture (Grimmelmann, 2008). It makes information sharing can be so easy as the social networking sites can disclose demographic information, update status, share emotions and put thoughts, post photos and videos, and share personal interest as well as leave comments on friends' timeline (Feng and Xie, 2014). The study by Pesce, et al. (2012) on tagging that is one of the popular features on Facebook have found that users might unknowingly reveal certain kinds of personal information that malicious attackers could profit from it to perpetrate significant privacy breaches. In their paper, Pesce, et al. (2012) conducted quantitative measurement on how the act of tagging pictures on Facebook could reveal private user attributes that are extremely sensitive. Given that there are risks associated in using the social networking sites, some users seem tolerable to this condition. This is shown in the study by Govani and Pashley (2005) as cited in Tuunainen et al. (2009) towards the university students as the respondents. They found that majority of the students are indeed aware of possible consequences of providing personally identifiable information to an entire university population (such as, risk of identity theft or stalking), but nevertheless, feel comfortable enough in providing their personal information.

Meanwhile, Liu et al. (2011) conduct the study related with the privacy concern, but focus on the disparity between the desired and actual privacy settings, and quantifying the magnitude of the problem of managing privacy. From their study, it was found that 36% of content remains shared with the default privacy settings. They also found that privacy settings match users' expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected. Thus, Liu et al. (2011) also explored how the results had the potential to assist users in selecting appropriate privacy settings by examining the user-created friend lists and suggested that information from the social network may be helpful in implementing new tools for managing privacy. According to Westin (1968), privacy is defined

as the desire of people to have the freedom of choice under whatever circumstances and to whatever extent they expose their attitude and behaviour to others. When applying to the social networking sites, privacy concern refers to the user's perception of the likelihood that their confidential information will be protected from unauthorized use or disclosure (Salleh and Hussein, 2011).

Facebook allows users to change their personal settings to control who can view their profile and what other information is viewable (Waters and Ackerman, 2011). The Facebook privacy management currently is mainly based on individual settings rather than group oriented settings on shared items such as pictures (Borneo and Barkhuus, 2011). Users can still communicate and share information on Facebook, but still can maintain their privacy by permitting only a selected audience upon the shared information. A study by Acquisti, and Gross (2006) concludes that generally the users do not know much about privacy settings and who can access the information they share. It seems that users have high trust on Facebook and assume that their information is safe and not realise about the Facebook's default privacy settings at open stage where it assumes users might want to share the information broadly (Borneo and Barkhuus, 2011). If users are overlooked this point, they will end up in a situation where all information either which to keep secret or publicly viewed would be exposed. According to Borneo and Barkhuus (2011), privacy is not only about managing and protecting information from unintended receivers but also how the information is used and interpreted by social ties.

Students and adolescent are among the most prolific users of social networking sites. Users in this age often appear to be neglecting the privacy matters. Several researchers such as Acquisti and Gross (2006) and Stutzman's (2006) argue that there is often a disconnect between students' desire to protect privacy and their behaviours. Meanwhile Waters and Ackerman (2011) found that students were motivated to use Facebook because they perceived their relationships improved with friends and family, although using Facebook could become negatively habit forming. Since students and young adults still in the process of developing their own identities, the social networking sites are capable to be a good platform (Ahn, 2011). Users will decide what to place on their profiles and what friends to display for others to see. This gives a picture that individuals make explicit decisions about disclosing information on their profile and their network provide social interactions towards the profile displayed (Ahn, 2011). This process of developing an identity is quite important since they are experiencing the phase of rapid growth and self-development process. Despite the supportive environment for social development, one should also consider the potential risks arise when the social networking sites were used in an overwhelming and uncontrollable manner. For example, students and adolescents are potentially exposed to the risks such as blackmail, cyber bullying and even sexual harassment (Ahn, 2011).

There are some researches focusing on the relationship between the demographic factors and the privacy concern. Findings from Feng and Xie (2014) had indicated that there was non-significant relationship between gender and teens' level of privacy concern. Chang and Heo (2014) also found that gender difference would not affect Facebook users' self-disclosure of "sensitive" and "highly sensitive" information. Fogel and Nehmad (2009) in their studies shown that general privacy concerns and identity information disclosure concerns are of greater concern to woman than men. However, there are greater percentages of disclosure of phone numbers and home addresses among men than women.

The research by Salleh and Hussein (2011) investigate how far the users aware of information privacy and disclosure on using social networking sites. In their study, they provide a framework that could be used to understand users' protective behaviour in relation to information disclosure. The framework was conceptualized based on the Protection and Motivation Theory (PMT) incorporated with other supporting factors that are believed can explain users' perception of privacy and security awareness in using social networking sites. To explain the proposed framework, Salleh and Hussein (2011) asserted that, higher privacy concern may be determined by higher perceived vulnerability associated with information



disclosure. This means that, when users perceived their information are misused by third parties, they tend to reduce the disclosure of their personal information on the internet. Other than that, Salleh and Hussein (2011) also mentioned that trust and perceived risk is believed to have an influence on personal information disclosure on social networking sites. Other researchers also put an interest when talking about trust, such as Dwyer, Hiltz, and Passerini (2007) argued that trust and usage goals may affect what people are willing to share. This is because Facebook users expressed greater trust in Facebook than MySpace users did on MySpace and thus were more willing to share information on the site (Boyd and Ellison, 2007). Within this context, it can be said that Facebook has a greater influence than the other social networking sites till they even can take for granted about privacy matters. This also supported by Jones and Soltren (2005) claimed that that users practice poor privacy control of their information while the third parties were consistently trying to obtain users' information.

In addressing the privacy management issue, Gummadi (2013) has outline several problems related to privacy management in using the social networking sites. As such, there is a lack of proper access control mechanism where it is regarded as primitive and often insufficient to capture the user intent. To explain further, Gummadi (2013) clarify that data sharing in social networks tend to overlap and involve the ever-changing social relationship. Gummadi (2013) also add that, users nowadays often not understand the implications of their actions and access of control settings. For example the complexities of Facebook privacy settings tend to make users to confuse and somehow make them to ignore and let the default privacy settings. As a result, different social networking applications and other users might get access to the personal information and data in such a way that is unexpected.

### 3. Research Methodology

The total respondent comprised 167 students, which all final semester students at Fakulti Pengurusan Perniagaan UiTM Pahang, which included the Diploma in Business Studies, Diploma in Banking and the Diploma Office Management. Out of 167 questionnaires distributed, only 112 questionnaires were usable for this study. The questionnaire form consists 2 parts; part A asked respondent's profile while part B asked about Facebook usage behaviour and Facebook privacy management. The questionnaire items used in this study were primarily adapted from previous studies. The items for individual privacy management and privacy control were adapted from Wolf et al. (2014). Respondents were asked to rate each item on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

The questionnaire was completed by the students during the class period on the date the survey was circulated. The data from the questionnaire were analysed using the Statistical Package for Social Sciences (SPSS), version 21.0. Descriptive statistics were analyzed to measure the frequencies of the demographic profiles. Descriptive measures such as the mean and standard deviation were used to examine the Facebook usage behaviour and individual privacy management. This study also employed the t-test to analyze the difference between two selected groups.

### 4. Findings

#### *Demographic profiles*

Table 1 shows the demographic profiles of the respondents. A total of 167 questionnaires were administered to the students of Faculty of Business Management, UiTM Pahang and 112 responded that contributed to a 67 percent response rate. As presented in Table 1, the majority of the respondents are the students of Diploma in Business Studies (41.1%). The highest percentage of respondents came from the age group of 20 to 21 years (93.7%) and

female students dominated the number of respondents as they represented 87 out 112 students (77.3%). It showed that, most of the respondents' CGPA were between 3.00 to 3.49 (49.5%).

**Table 1.** Demographic Profiles

Personal Demographic Variables	Categories	Frequency	%
Programme	BM111	46	41.1
	BM112	29	25.9
	BM118	37	33.0
Gender	Male	25	22.7
	Female	87	77.3
Age	20-21 years	105	93.7
	22-23 years	6	5.4
	24 years and above	1	0.9
CGPA	3.50 and Above	36	32.4
	3.00 - 3.49	56	49.5
	2.50 - 2.99	19	17.1
	2.00 - 2.49	1	0.9
Total		112	100

#### *Facebook usage behavior*

From Table 2, it shows that 86 out of 112 respondents are not addicted to Facebook (76.8%). Most of the respondents were Facebooking twice a day (43.2%) while 44 of the respondents (39.6%) were Facebooking once a week, 12 of the respondents (10.8%) Facebooking every 30 minutes and the remaining (6.3%) were Facebooking every minutes. As presented, 89 (79.5%) of the respondents were using smartphone to access the Facebook, 13 of them (11.6%) were using PC, and 5 of the respondents (4.5%) used tablet and others. The data showed that majority of the respondents were using Facebook for more than 2 years (92.9%), 5 (4.5%) have used Facebook for 1 to 2 years, and 3 (2.7%) less than a year.

**Table 2.** Facebook Behaviour

Facebook Behaviour	Categories	Frequency	%
Addicted to Facebook	Yes	26	23.2
	No	86	76.8
Frequency for Facebooking/Online	Every minutes	7	6.3
	Every 30 minutes	12	10.8
	Twice a day	49	43.2
	Once a week	44	39.6
Accessing Facebook	Smartphone	89	79.5
	PC	13	11.6
	Tablet	5	4.5
	Others	5	4.5
Period using Facebook	Less than a year	3	2.7
	1 to 2 years	5	4.5
	More than 2 years	104	92.9
Total		112	100

The motives of using Facebook is shown in Figure 1. The pie chart indicates that 48 per cent of students used Facebook to maintain relationship with friends. Respondents were also likely to use Facebook to join group such as group for their class and University's club with the

percentage of 18 percent. Besides that, the respondents were also used Facebook for meeting new people (13%), for business purpose (10%), others (6%), and for playing games or use applications (5%).

Facebook users have few options on how they access to the internet. The questionnaire data in Figure 2 shows that most of the respondents (35%) access to the internet by subscribing prepaid internet plan. This include variety of network coverage offered such as Hotlink, Celcom, Digi and others. Respondents were also had chosen free Wi-Fi (32%) to access the internet. While the remaining used broadband (21%) and subscribing the post-paid internet plan (12 %). When it comes to privacy awareness, it was discovered in Figure 3, 95.5 percent of the students were aware with the privacy settings in Facebook. They knew that they can change their privacy settings in Facebook. From the results it shows that, the respondents' level of awareness about privacy settings is high. While 4.5 percent of the respondents were not aware about the privacy settings in Facebook.

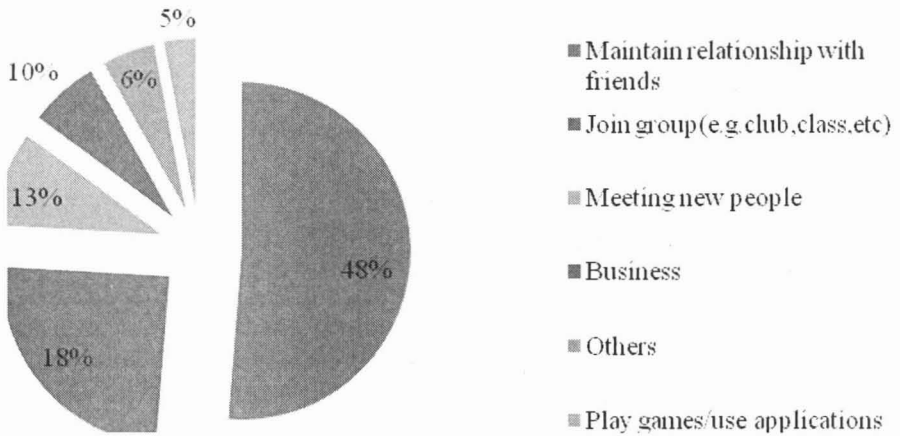


Fig. 1 Motives of using Facebook

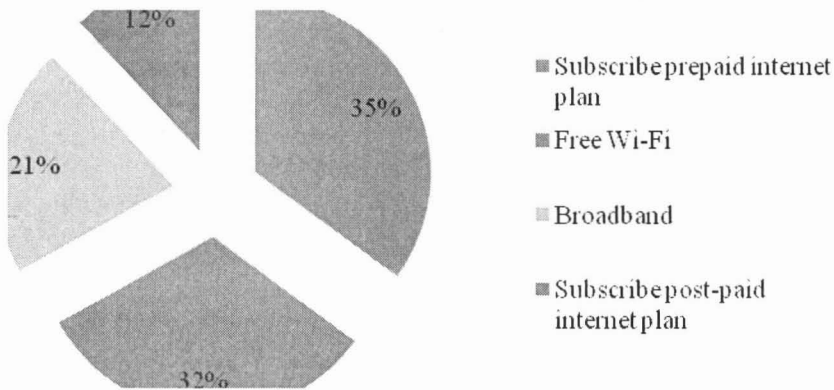
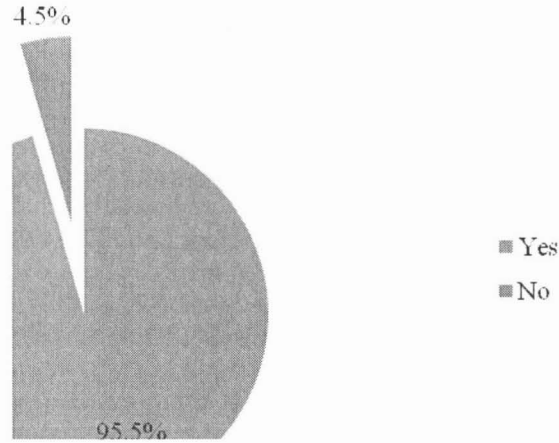


Fig. 2 Access to the internet



**Fig. 3** Awareness of privacy settings in Facebook

*Mean Analysis for Individual Privacy Management*

Table 3 indicates the mean score for each item in Individual Privacy Management variable. The result of mean score is arranged from highest score to the lowest score. The highest mean score is statement “careful to accept friend requests” at mean value of 4.46. It shows that the respondents are make hard decision to accept friend requests especially from the strangers. Next, the respondents choose statement “only post suitable information for everyone to see” as second highest mean score at 4.32. The respondents are careful to choose the appropriate information before post it on the Facebook. Then, the third highest mean score is 4.25, where the respondents do not fill in all information that is requested by Facebook. By doing so, the respondents can ensure that their privacy could be protected. Next, is the respondents will make sure that only friends can see their profile on Facebook with 4.24 mean score. Therefore, the personal information is safe from strangers or any random visitors to the profile. Some respondents would untag themselves from any inappropriate photos at fifth place with 4.23 mean score. Other items recorded less that 4.00 of mean score as presented in table 3.

**Table 3.** The mean score for Individual Privacy Management

Items	Mean
Careful to accept friend requests	4.46
Only post suitable information for everyone to see	4.32
Do not fill in all the information that is requested by Facebook	4.25
Only friends can see my profile	4.24
Untag myself from photos I find inappropriate	4.23
When install an application, make sure that I am the only who can see	4.03
Make use of private message when talk about sensitive subjects	3.84
Review photos friends tag, before appear on my timeline	3.81
Make use of Facebook lists when posting information	3.80
Defriend those I longer want to see my status updates	3.67



Mean Analysis for Privacy Control

The result of mean score for Privacy Control is presented in table 4. As presented in the previous table, the mean score is arranged from highest score to the lowest score. All items for Privacy Control is recorded bigger than 4.00 mean value. The highest score is 4.58 where the respondents worried to place or post any information that could embarrass them in Facebook. It shows that the respondents are careful to choose suitable photos or any information before upload or post it. Next, the respondents are worried that others will find private information about them on Facebook with a mean score of 4.47. Therefore, they have to select certain information and not easily post any private information. Then, the respondents also worried about posting any information on Facebook because it might be used in ways they had not foreseen with 4.28 mean score. Lastly, two items that are closely related to each other is at fourth and fifth place with 4.27 and 4.25 mean score respectively. The details result is shown in table 4.

**Table 4.**The mean score for Privacy Control

Items	Mean
I am worried about others placing embarrassing information about me on Facebook	4.58
I am worried that others find private information about me in Facebook	4.47
I am worried about posting information in Facebook, because it might be used in ways I had not foreseen	4.28
I am worried that others misuse the information I post in Facebook	4.27
I am worried about posting information in Facebook, because of what others might do with it	4.25

T-Test Analysis

The t-test analysis is used in order to find the different mean between two groups regarding the same issue. Table 5 indicates the difference between gender for both variables. The result showed that there is no significant difference between male and female respondents regarding Individual Privacy Management. Meanwhile, there is a significant difference between male and female on privacy control. The t-value is -2.153 and the p-value is 0.038 showed that female respondent is significantly more concern on privacy control with mean value is 4.437.

**Table 5.**T-test on Gender

Variable	Male	Female	t-value	p-value
Individual Privacy Management	3.888 (0.536)	4.111 (0.519)	-1.885	0.062
Privacy control	4.092 (0.731)	4.437 (0.611)	-2.153	0.038*

Next, this study also investigates the difference between respondents who do aware on privacy setting as provided by Facebook. Figure 3 reported that majority of the respondents are aware of privacy setting provided by Facebook at 95.5 percent. However, the t-test analysis shows that there is no significant difference between those who are aware about privacy setting and who aren't. For both variables; the Individual Privacy management and Privacy control

either the respondents aware or not aware about the privacy setting it does not affect the perception on both variables. The detail result is presented in the following table.

**Table 6.**T-test on Awareness of Privacy Setting

Variable	Yes	No	t-value	p-value
Individual Privacy Management	4.069 (0.530)	3.953 (0.459)	-0.481	0.631
Privacy control	4.369 (0.661)	4.320 (0.363)	-0.165	0.870

## 5. Conclusion and Recommendation

Digital privacy has been a consistent concern since the Internet became a popular medium in the 1990s (Marwick et al., 2010). Information sharing can be so easy as social media users such as Facebook can disclose demographic information, update status, share emotions and put thoughts, post photos and videos, and share personal interest as well as leave comments on friends' timeline (Feng and Xie, 2014). Therefore, the privacy management becomes crucial to those who are heavily using the internet like social media. The findings of this showed that the awareness level on privacy setting is high among the youth. Majority of them are aware about that privacy service offered by Facebook. As 48 percent of the respondents use Facebook to maintain the relationship with family members and friends, they were careful to accept any friend request. Then, they also concern to post only suitable information for everyone and they prefer not to fill in all personal information asked by Facebook. These three items were selected as the highest mean score for individual privacy management variable. While for privacy control, the respondents worried that other people may post something embarrassing about them on Facebook. The respondents were also worried that other people may find private information about them on Facebook as the possibility of a stranger to do so is very high. So that, it is recommended to every Facebook user to make use the privacy setting by setting the group list and post any information to the selected group only.

The t-test results show that both male and female respondents are aware on privacy management and There is no difference in both groups. This result is consistent with the study by Chang and Heo (2014) indicate that both gender difference would not affect the user privacy management. However, there is a difference between female and male for privacy control. Anyway, as the majority of the respondents are aware about the privacy setting, the result shows there is no significant difference between those who are aware and those who are not aware for both variables. The gender difference analysis is recommended for future study as many previous studies done before indicated that gender would react differently on privacy management as found by Fogel and Nehmad (2009). In future, this study could be extended to explore the relationship between user behavior to privacy management and privacy control. It is meaningful to conduct this study for larger numbers of respondents and also include the non student respondents.

## 6. References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Proceedings of 6<sup>th</sup> Workshop on Privacy Enhancing Technologies* (pp. 36-58). Cambridge, UK: Robinson College.

- Ahn, J. (2011). The Effect of Social Network Sites on Adolescents' Social and Academic Development: Current Theories and Controversies. *Journal Of The American Society For Information Science And Technology*, Vol. 62, No. 8, pp. 1435–1445.
- Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, Vol. 13, Issue 1, p210-230, Blackwell.
- Boyd, D., & Hargittai, E.(2010). Facebook Privacy Settings: Who Cares?. *First Monday* 15 (8).
- Bornoe, N., & Barkhuus, L. (2011). Privacy Management in a Connected World: Students' Perception of Facebook Privacy Settings. *Workshop on Collaborative Privacy Practices in Social Media, CSCW 2011*, Hangzhou, China.
- Chang, C.W., & Heo, J. (2014). Visiting Theories That Predict College Students' Self-disclosure on Facebook. *Computers in Human Behavior* 30, pp 79-86.
- Chen, G. (2012). The impact of new media on intercultural communication in global context. *China Media Research*, 8(2), Retrieved from <http://www.chinamediaresearch.net>.
- Cheng, Y., Park, J., & Sandhu, R. (2013). Preserving User Privacy from Third-party Applications in Online Social Networks. *International World Wide Web Conference Committee*.
- Croft, C. (2007). A Brief History of The Facebook. Retrieved from <http://charlenegagnon.files.wordpress.com/2008/02/a-brief-history-of-the-facebook.pdf>.
- Debatin, B., Lovejoy, J.P., Horn, A.K., & Hughes, B.N. (2009). Facebook and Online Privacy : Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, Vol.15, pp 83-108.
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of AMCIS 2007*, Keystone, CO.  
Retrieved from <http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf>.
- Feng, Y., & Xie, W. (2014). Teens' Concern for Privacy When Using Social Networking Sites:An analysis of Socialization Agents and Relationships with Privacy-protecting Behaviors. *Computers in Human Behaviour*, 33, pp 153-162.
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computer in Human Behavior*, Vol 25 pp. 153–160 doi:10.1016/j.chb.2008.08.006.
- Grimmelmann, J. (2008). Facebook and the Social Dynamics of Privacy. Retrieved from [http://works.bepress.com/james\\_grimmelmann/27/](http://works.bepress.com/james_grimmelmann/27/).
- Gummadi, K. P. (2013). *Addressing the Privacy Management Crisis in Online Social Networks*. WWW 2013 Companion, Rio de Janeiro, Brazil.
- Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. *Project MAC: MIT Project on Mathematics and Computing*. Retrieved from <http://www-swiss.ai.mit.edu/6.805/studentpapers/fall05-papers/facebook.pdf>.
- Liu, Y., Krishna, P., Gummadi, Krishnamurthy, B., & Alan Mislove (2011). Analyzing Facebook privacy settings: user expectations vs. Reality. *IMC '11 Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, pp. 61-70.
- Marwick, A. E., Diaz, D. M., & Palfrey, J. (2010). Youth, Privacy, and Reputation, Public Law & Legal Theory Working Paper Series. Paper No. 10-29.
- Pesce, J. P., Las Casas, D., Rauber, G., & Almeida, V (2012). Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook. *PSOSM '12 Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, Article No. 4.
- Robert, Lee, K. (n.d.). Impacts of Information Technology on Society in the new Century. Retrieved from <http://www.zurich.ibm.com/pdf/news/Konsbruck.pdf>.
- Sophos, Inc. (2013). Security Threat Report 2013: New Platforms and Changing Threats, *Security Threat Report 2013*.
- Squicciarini, A. C. Shehab, M., & Paci, F. (2009). Collective Privacy Management in Social Networks, *Track: Security and Privacy / Session: Web Privacy*, pp 521-530.

- Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *Journal of the International Digital Media and Arts Association*, 3 (1), 10-18.
- Salleh, N., & Hussein, R. (2011). Information Disclosure Behaviour in Social Media among Malaysian Youth: The impact of Privacy Concern, Risk and Trust. *Symposium on Information & Computer Sciences (ICS 2011)*.
- Stutzman, F., & Kramer-Duffield, J. (2010). Friends Only : Examining a Privacy-Enhancing Behavior in Facebook, *CHI 2010 : Privacy*, April 10-15,2010, Atlanta, Ga, USA.
- Tuunainen, V.,K., Pitkanen, O., & Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking sites – Case Facebook. *22<sup>nd</sup> Bled eConference eEnablement:Facilitating an Open, Effective and Representative eSociety*, June 14-17 2009, Bled, Slovenia.
- Waters, S., & Ackerman, J. (2011). Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure. *Journal of Computer-Mediated Communication*, Issue 17, pp. 101–115. doi:10.1111/j.1083-6101.2011.01559.
- Westin, A. (1968). Privacy and Freedom. 25 Washington and Lee Law Review. 166, Retrieved from <http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>
- Wolf, R.D., Willauert, K., & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computer in Human Behavior*, 35, pp. 444-454. doi.org/10.1016/j.chb.2014.03.010.
- Wooley, S. (2013). Constantly Connected: The Impact of Social Media and the Advancement in Technology on the Study Abroad Experience. *The Elon Journal of Undergraduate Research in Communications*, Vol. 4, No. 2, pp 40-50.