

# DATA SECURITY, CONTROL AND PRIVACY MANAGEMENT OF FACEBOOK USAGE AMONG UNDERGRADUATE STUDENTS

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

<sup>1</sup>Faculty of Accountancy, Universiti Teknologi MARA, 42300 Bandar Puncak Alam, Selangor, Malaysia.

<sup>2, 3, 4</sup> Faculty of Business Management, Universiti Teknologi MARA, 26400 Bandar Jengka, Pahang, Malaysia.

<sup>1</sup>ridhuan@salam.uitm.edu.my; <sup>2</sup>alhudatajuddin583@pahang.uitm.edu.my;  
<sup>3</sup>izzatibahsri@pahang.uitm.edu.my; <sup>4</sup>Zarira2939@pahang.uitm.edu.my

## ABSTRACT

*Facebook is one of the most popular social networking sites with millions of users around the globe. However, most users overlooked their privacy management where their personal information are exposed and might be misused by others. This study was conducted on 290 respondents on a particular university regarding their Facebook usage upon data security and privacy control. A non-experimental research, particularly descriptive research and correlational research were applied in order to identify whether privacy and data security concerns, perceived privacy control and privacy concerns have a relationship with individual privacy management. Majority (91%) respondents have been using Facebook for more than 2 years, but most of them were not addicted to it. Maintaining relationship with friends and family members were the main reason why the respondents use Facebook. Other reasons given are to join a specific class group or club, to read news, to get the latest information and current issues. The regression analysis shows all hypotheses were supported in which every unit increase in independent variables will increase the dependent variable, while correlation indicated a positive relationship between privacy and data security concerns (PDSC) on Facebook  $r = .385$ , and perceived privacy control (PPC)  $r = .487$ , with individual privacy management. Privacy concern (PC) showed a moderate positive relationship as represented  $r = .577$ .*

**Keywords:** Facebook; data privacy control; privacy management; privacy and data security concerns; privacy concern.

## 1. INTRODUCTION

Facebook is a social network site, co-founded by Mark Zuckerberg with his college roommates and fellow Harvard University students in the year 2004 as a way for college and university students to keep in touch when they leave campus (Croft, 2007). According to Boyd and Ellison (2007, p.211) cited in Westermann (2011, p.1), Social Network Site (SNS)

is defined as “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.” There are various SNSs such as Myspace, Friendster, Twitter, Line, WhatsApp, Instagram and the most popular today is Facebook. These SNSs are used as channels for people around the world to communicate. Since they are free and only require a person above the age of 13 with a valid e-mail address to register, almost everyone can enjoy using this social networking media for different activities. It allows people to exchange information, share photos and videos, and business activities. In fact, the major users of social networking media are teenagers, young adults as well as the university students (Borneo & Barkhuus, 2011).

At present, Facebook has evolved and become the largest SNS in the world and worth billions of dollars of investments. People around the world are sharing content and communicating with each other from different parts of the globe. Facebook is available in 37 different languages. It have public or basic features such as ‘marketplace’, ‘groups’, ‘events’, ‘pages’, and ‘presence technology’. Other networking components featured on Facebook are the ‘wall’, ‘photo album’, ‘status updates’, ‘microblogging’, ‘newsfeed’ and other numerous components for its users. According to Borneo and Barkhuus (2011), millions of Facebook users are befriending each other through explicit social ties where they can passively go through the newsfeed and browse their friend’s profile. The features provided by Facebook make social networking less complicated because users can share their information or interests with others.

Facebook enables users to create profile page where they can upload their personal information and contact details. Furthermore, users can also share their locations and with whom they are currently with. This kind of information is sufficient enough to expose Facebook’s users to potential criminal victims. The information posted on Facebook especially ones that are related to personal information such as address, phone number, pictures, account numbers are easy target of 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 spread computer viruses, malware and even spam messages through the fake web address link (Sophos Inc. 2013). Therefore, it is important for users to be aware of their privacy settings and be precautious when sharing information. Although Facebook has provided the privacy settings, users may overlook and not apply it.

The issue of privacy and social networking media have received 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 problems on privacy concerns also emerged when various social networking media including Facebook launched the social networking platform that allows third party developers to contribute applications and widgets as some additional functions (Cheng, Park, & Sandhu, 2013). Although they have legal rights since both the social networking media and the third party developers have commercial benefits, users still face risks when their personal information are exposed to violation. Other than that, Facebook users will also receive lots of information from their online activities using this social media. The worrying part is not all the information is true or inclusive (Lee, n.d.). Some users may also post information on sensitive issues as well as personal ones too. This happens because

they are unaware or make deliberate attempts and underestimate the safety risks on Facebook (Venkat, Pichandy, Barclay & Jayaseelan, 2014). This paper will investigate the relationship between independent variables which include; privacy and data security concerns, privacy concern, and perceived privacy control with the dependent variable, an individual privacy management. All these relationships will be presented in detail under the research methodology section.

## **2. LITERATURE REVIEW**

Privacy settings are useful to those who share information so that account owners are able to manage the accessibility to their personal information (Boyd & Hargittai, 2010). According to Westin (1968), privacy is defined as the people's desire to have the freedom of choice under whatever circumstances and to whatever extent they expose their attitude and behaviour to others. Based on 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 & Hussein, 2011). Digital privacy has been a consistent concern since the Internet became a popular medium in the 1990s (Marwick, Diaz, & Palfrey, 2010). Facebook and other social networking sites have indeed provided the privacy settings for all their users. However, it is still speculative whether the privacy settings provided by these social networking sites really secure the user's privacy.

Somehow, the users themselves are not concerned with their privacy information when using the Internet. Debatin, Lovejoy, Horn, and Hughes (2009) found that Facebook users do not change their default privacy settings and rely on lax, initial start-up settings. In fact, even if the user's awareness level on privacy is above average and manages privacy settings of his or her profile, they still face threats including hacking and bugs (Venkat et al., 2014). On the other hand, Hassan and Akhtar (2010) analysed some Facebook games and investigated their negative effects on the social wellbeing of users. They concluded that, particular segment of the computer gaming industry that manifests itself through Facebook is not as transparent as it might seem. This is because of the involvement of multiple parties in the entire gaming process including the game developer, the advertiser and the end user. Users might be cheated or manipulated into tricky transactions that they may not realize (Hassan & Akhtar, 2010).

Wisniewski, Knijnenburg and Lipford (2014) has categorized the privacy concerns among users into six different categories or classes which are 1) privacy maximizers; 2) selective sharers; 3) privacy balancers; 4) self-censors; 5) time savers/consumers; and 6) privacy minimalists. Each of these classes of privacy concerns users to demonstrate a distinctly multidimensional pattern of privacy management strategies. For example, "self-censors could arguably be leveraging a coping strategy to protect their personal privacy by reducing self-disclosures" (Wisniewski et al. 2014, p. 5). The results from Wisniewski et al. (2014) shed some ideas that most users do not simply employ more or fewer privacy behaviours. It also might indicate that each user has their individual perspective about privacy management and it can be measured according to a certain degree. Meanwhile, Squicciarini, Xu, and Zhang (2010) proposed a tool called Collaborative Privacy Management (CoPE) to help users manage their personal information shared within a social network. It focuses on supporting the management of the access rights for digital images, and provides functions such as Potential Co-managed Photos Notification; Stakeholder Request; Photo Access Management; and Track Viewing History (Squicciarini et al. 2010). The approach proposed by Squicciarini

et al. (2010) will enhance the privacy management tools for Facebook users by introducing the collaborative privacy management model. In this model it allows two or more users' preferences of privacy settings to be interpreted into one privacy setting. Although this approach is more to image related privacy, however the authors are looking forward to generalize it to other contents as well.

In addressing the privacy management issue, Gummadi (2013) has outlined 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's intention. To explain further, Gummadi (2013) clarified that data sharing in social networks tend to overlap and involve the ever changing social relationship. He also added that, users nowadays often do not understand the implications of their actions and access of control settings. For example the complexities of Facebook privacy settings tend to confuse users and somehow make them agree to the default privacy settings. As a result, different social networking applications and other users might get access to the personal information and data in unexpected ways.

The findings by Gummadi (2013) is significant with the study by Venkat et al. (2014) which revealed that Facebook users have inadequate levels of knowledge and awareness about privacy and Facebook settings. They also discovered that there is a marked difference between the perceived and actual privacy settings due to which privacy management is poorly maintained by the users. It also indicates that, users' personal information are exposed publicly where other users can view those information and use it for malicious intentions. Venkat et al. (2014) also found that users often have misconceptions about the privacy settings where they think that only their friend's lists can view their posts, updates and photographs.

Another study from Liu, Krishna, Gummadi, Krishnamurthy and Mislove (2011) on privacy concern focused on the disparity between the desired and actual privacy settings, and quantifying the magnitude of the problem of managing privacy found that 36% of content remains are 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. 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.

In another view, the privacy and data security concerns is related to the individual behaviour in dealing with the privacy and data protection since every individual have a right to get protection of personal information as a fundamental freedom. 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.

A study by Acquisti, and Gross (2006) concluded that generally users do not know much about privacy settings and who can access the information they share. Users tend to have high trust on Facebook and assume that their information is safe and do not realize about the Facebook's default privacy settings which is at open stage where it assumes users might want to share the information broadly (Bornoe & Barkhuus, 2011).

### 3. RESEARCH DESIGN

This study used non-experimental research, namely descriptive research and correlational research. In this research, the respondents were undergraduates in their final semester. The research framework is shown in Figure 1.

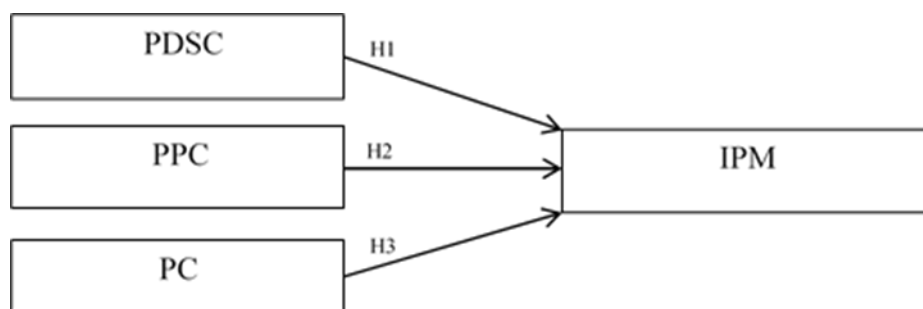


Figure 1: The theoretical framework.

- H1: Privacy and data security concerns (PDSC) on Facebook has a positive relationship on individual privacy management (IPM).
- H2: Perceived privacy control (PPC) has a positive relationship on individual privacy management (IPM).
- H3: Privacy concern (PC) has a positive relationship on individual privacy management (IPM).

### 4. METHODOLOGY

The instrument used for the data collection was a survey questionnaire adapted from Wolf, Willaert and Pierson (2014). A total of 350 sets of questionnaires were distributed to the undergraduate students and 290 sets were returned for further analysis (82.9% response rate). Apart from closed ended questions, respondents were also asked to rate each item on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The questionnaire contained 3 parts, Part A focused on respondents' profile, part B on Facebook usage and Part C on the variables studied which include IPM, PC, PPC and PDSC. The breakdown of each section in the questionnaire is shown in Table 1.



Table 1: Instrument section.

Part A	Respondents' Profile	Closed-ended question	Descriptive statistics
Part B	Facebook Usage	Closed-ended question	Descriptive statistics
Part C	Individual Privacy Management (IPM)	5-point Likert Scale (based on level of agreement)	Ordinal
	Privacy Concern (PC)	5-point Likert Scale (based on level of agreement)	Ordinal
	Perceived Privacy Control (PPC)	5-point Likert Scale (based on level of agreement)	Ordinal
	Privacy and Data Security Concerns on Facebook (PDSC)	5-point Likert Scale (based on level of agreement)	Ordinal

The data from the questionnaire was analysed using the Statistical Package for Social Sciences (SPSS), version 22.0. Descriptive measures such as the mean and standard deviation were used to examine the Facebook usage behaviour and t-test analysis was conducted to study the difference between groups. All constructed questions used as measurements were checked for their reliability. Reliability of scales was calculated using Cronbach's  $\alpha$  as shown in Table 2. From the table it is shown that the reliability coefficient for the instrument were acceptable, where the individual privacy management recorded  $\alpha$  0.745, privacy control ( $\alpha$  0.864), perceived privacy control ( $\alpha$  0.859), privacy and data security concerns on Facebook ( $\alpha$  0.597). Other than that, this research also applied the correlation and regression analysis to examine the relationship between the variables.

Table 2: Reliability result for Cronbach's Alpha (Goodness of the Data).

	Reliability Result (Cronbach's Alpha)	No. of Items
IPM	$\alpha$ 0.745	10
PDSC	$\alpha$ 0.597	5
PPC	$\alpha$ 0.859	4
PC	$\alpha$ 0.864	5

## 5. FINDINGS AND DISCUSSION

### 5.1 Demographic Data and Facebook Usage

This study was conducted at a university where majority of the students use Facebook or have Facebook accounts. Table 3 presents the demographic data. The total number of respondents are 290 where majority of them were female (66.7%), and another 33.3% were male students. Ninety four percent of the respondents' age ranged from 20 to 21 years old which is the age group for undergraduate university students.

Table 3: Demographic data of the respondents.

<i>Variables</i>	<i>Categories</i>	<i>Frequency</i>	<i>%</i>
Gender	Male	96	33.3
	Female	192	66.7
Age	18-19 years	1	0.3
	20-21 years	271	94.1
	22-23 years	12	4.2
	24 years and above	4	1.4
		N = 290	100

This study also explored the frequency of the respondents when using Facebook. A detailed result is tabulated in Table 4 where 50% admitted that they logged into Facebook once a week, while 37.9% logged in twice a day. Other respondents admitted to logged into Facebook every 30 minutes (8.3%) and 3.5% logged in every minute. It was revealed that a majority (91%) of respondents have been using Facebook for more than 2 years, but it also showed that most of them were not addicted to Facebook. Maintaining relationship with friends and family members were found to be the main reason why the respondents use Facebook with a percentage of 76.6. This is consistent with Mazman and Usluel (2011) who discovered that, generally people use Facebook to maintain the existing relationship. Meanwhile, 32.1% use Facebook to join a specific class group or club, meeting new people (22.1%), playing games or business purposes (14.1%). The respondents also used Facebook for other reasons such as to read news, get the latest information and current issues which can easily be found in the News feed function.

Table 4: Usage of the Facebook.

<i>Variables</i>	<i>Categories</i>	<i>Frequency</i>	<i>%</i>
Frequency to access Facebook	Every minute	10	3.5
	Every 30 minutes	24	8.3
	Twice a day	110	37.9
	Once a week	144	50.0
Tools/Medium to access Facebook	Smartphone	206	71.0
	PC	59	20.3
	Tablet	11	3.8
	Others	14	4.8
Period of using Facebook	Less than a year	5	1.7
	1 to 2 years	21	7.2
	More than 2 years	264	91.0
Addicted to Facebook	Yes	74	25.5
	No	216	74.5
Internet access	Prepaid	138	47.6%
	WIFI	135	46.6%
	Broadband	86	29.7%
	Postpaid	38	13.1%
Purpose of using Facebook	Maintain relationship with friends and family	222	76.6%
	Join group (e.g. Club, class, etc.)	93	32.1%
	Meeting new people	64	22.1%
	Play games or use applications	41	14.1%
	Business purpose (online shopping or selling)	41	14.1%
	Others	30	10.3%
		N = 290	100

## 5.2 T-test Analysis

Table 5 indicates the difference between genders for all variables. The results showed that there were no significant difference between male and female respondents regarding individual privacy management, privacy and data security concerns, and perceived privacy control, on Facebook. Nevertheless, there was a significant difference between male and female on privacy concern at the significant level of 0.029. Our findings is somewhat similar with the study from Grubbs and Milne (2010), Kuo and Tang (2015) who discovered that females have higher degree of privacy concern and protection than the males.



Table 5: T-test on gender.

Variable	Male	Female	t-value	Sig.
IPM	3.652 (0.649)	4.042 (0.535)	-5.429	0.218
PDSC	3.450 (0.635)	3.759 (0.566)	-4.194	0.241
PPC	3.719 (0.794)	4.119 (0.727)	-4.274	0.150
PC	3.894 (0.756)	4.341 (0.653)	-5.189	0.029*

\*Significant at p-value 0.05

This study also investigated the difference between respondents' awareness of privacy settings for all variables and the detailed results are presented in Table 6. The respondents' awareness of the privacy setting did not affect the perception of all variables. It is either the respondents are not fully aware about the importance of preserving their privacy information or they do have awareness about privacy policy but taken for granted (Govani and Pashley, 2005). It might also imply that, respondents might blindly believe that their personal information are in safe custody on Facebook (Venkat et al. 2014). Similarly, Mathiyalakan, Heilman and White (2013) also found that, their respondents tend to trust Facebook regarding the privacy and security concern, which might imply that they are naïve about privacy issues or it reflects a cultural bias.

Table 6: T-test on awareness of privacy settings.

Variable	Yes	No	t-value	Sig.
IPM	3.947 (0.576)	3.493 (0.782)	3.377	0.260
PDSC	3.668 (0.603)	3.486 (0.634)	1.328	0.726
PPC	3.993 (0.772)	3.881 (0.753)	0.642	0.873
PC	4.229 (0.712)	3.781 (0.707)	2.779	0.993

\*Significant at p-value 0.05

### 5.3 Correlation

In this study, Pearson Correlation Coefficient analysis was used to evaluate whether there was a linear relationship between variables in the population. The results in Table 7 revealed that there was a positive correlation on privacy and data security concerns on Facebook (PDSC)  $r = .385$ ,  $n = 290$  and perceived privacy control (PPC)  $r = .487$ ,  $n = 290$  with individual privacy management. While privacy concern showed a moderate positive relationship as represented  $r = .577$ ,  $n = 290$ . There is also a positive relationship among each variable. It suggested that the changes in one variable will also affect the changes in other variables. According to Pearson Correlation analysis, a greater individual privacy management is associated with a greater attention to improve the privacy and data security, privacy control and privacy concern.

Table 7: Pearson correlation among Construct.

Constructs	IPM	PDSC	PPC	PC
IPM	1.000	0.385**	0.487**	0.577**
PDSC		1.000	0.369**	0.391**
PPC			1.000	0.453**
PC				1.000

\*Significant at the 0.01 level

### 5.4 Regression Result

In order to perform hypotheses, multiple regression analyses were conducted to examine the relationship between the independent variables and dependent variables. The result indicated that in regression analysis, the R-square ( $R^2$ ) is 0.411. It was designated by 41.1% of the dependent variable is explained by the independent variables, whereas another 58.9% is not explained. Based on multiple linear regression analysis in Table 8, all hypotheses were supported.

As exhibited in the table, there were positive and significant effects among all three independent variables with the dependent variable. Hypothesis 1 examines the relationship between PDSC and IPM. The significant and positive relationship means with every unit increase in PDSC, the IPM will increase by 0.130 ( $\beta = 0.130$ ,  $p < 0.05$ ). Therefore, H1 was supported. Hypothesis 2 examines the relationship between PPC and IPM. A path coefficient of 0.198 which is significant at  $p < 0.05$ , specifies that every unit increased in PPC will increase IPM by 0.198. Thus, H2 was supported. Hypothesis 3 examines the relationship between PPC and IPM. A path coefficient of 0.345 which is significant at  $p < 0.05$ , specifies that every unit increased in PC will increase IPM by 0.345. Hence, H3 was supported.

Table 8: Results of hypothesis tests.

Model	R <sup>2</sup>	β	Sig.	Hypotheses Results
<b>Individual Privacy Management (IPM)</b>				
IPM = PDSC + PPC + PC	0.411			
(Constant)		1.201		
PDSC		0.130	0.010*	H1 was accepted
PPC		0.198	0.000*	H2 was accepted
PC		0.345	0.000*	H3 was accepted

\*Significant at *p*-value 0.05

$$IPM = \alpha + 0.130 PDSC + 0.198 PPC + 0.345 PC + e$$

## 6. CONCLUSION

Information sharing on Facebook can be as easy as disclosing demographic details updating status, sharing emotions and putting thoughts, posting photos and videos, and sharing personal interest as well as leaving comments on friends' timelines (Feng and Xie, 2014). Therefore, privacy management becomes crucial to those who heavily use the Internet like Facebook users. Currently, Facebook users are tested on their awareness on privacy and it could be seen that there was no difference between the aspect of genders as well as those who are aware on privacy settings.

This study examined three independents variables which hypothesised to influence the individual privacy management. All hypotheses used in this study were supported thereby indicated a positive and significant relationship between independent variables and dependent variable. However, there is more to do in order to instil the importance of managing privacy settings on Facebook properly. As disclosed in the findings, the respondents' awareness of the privacy setting did not affect the perception of all variables used in this study. It is expected that users should have more awareness about the importance of privacy especially when sharing information. Consequently, this study has important implications towards existing literatures about the privacy concern, data security, control and privacy management of Facebook usage among undergraduate students. On the other hand, it shed light to discover the applicable mechanism in strengthening the consciousness of social media users in which they need to actively manage their privacy information appropriately.

There are some limitations in this research as the respondents were youths from the diploma level aged between 20 to 21 years old. In order to have more colours on the results, future research should consider broader variant age of respondents. In addition, female respondents exceeded the male, thus it may have affected the magnitude of the result. Future studies may consider equal number of respondents among different genders to get equal representation of the results. Furthermore, the sample was based on only one university, hence the findings may not be applicable to account for all Facebook users in other universities at national or international level. In order to remedy this shortfall, the researcher plan to expand the generalised findings by replicating this study to several additional higher educational institutions to include larger samples and different demographic characteristics.

## 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*, 36-58. Cambridge, UK: Robinson College.
- Bornoe, N. and 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.
- Boyd, D., and Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication*, 13(1), 210-230, Blackwell.
- Boyd, D., and Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8). Available from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589>
- Cheng, Y., Park, J. and 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, and Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, *Journal of Computer-Mediated Communication*, 15, 83-108.
- Gummadi, K. P. (2013). Addressing the Privacy Management Crisis in Online Social Networks, *WWW 2013 Companion*, Rio de Janeiro, Brazil.
- Govani, T and Pashley, H. (2005). *Student Awareness of the Privacy Implications When Using Facebook*. Retrieved from <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>
- Grubbs, M., & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, 10(2), 28-45.
- Hassan, K. F., & Akhtar, M. S. (2010). *The Dark Side of Facebook Games*, Unpublished thesis, Worcester Polytechnic Institute.
- Kuo, T. & Tang, H. L. (2015). Gender Differences in Facebook's Privacy Settings, *Issues in Information Systems*, 16(1), 149-154.
- Lee, R. K. (n.d.). *Impacts of Information Technology on Society in the New Century*. Retrieved from <http://www.zurich.ibm.com/pdf/news/Konsbruck.pdf>
- Liu, Y., Krishna P. Gummadi, Krishnamurthy, B. and Alan Mislove (2011). Analyzing Facebook Privacy Settings: User Expectations vs. Reality, *IMC '11 Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 61-70.

- Marwick, A. E., Diaz, D. M., and Palfrey, J. (2010). Youth, Privacy, and Reputation, *Public Law & Legal Theory Working Paper Series*, Paper No. 10-29.
- Mathiyalakan, S., Heilman, G., and White, S. (2013). Gender Differences in Student Attitude toward Privacy in Facebook, *Communications of the IIMA*, 13(4), 35-42. Available at: <http://scholarworks.lib.csusb.edu/ciima/vol13/iss4/3>
- Mazman, S. G., & Usluel, Y. K. (2011). Gender differences in using social networks. *The Turkish Online Journal of Educational Technology*, 10(2), 133–139.
- Salleh, N. and 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)*.
- Sophos Inc. (2013). Security Threat Report 2013: New Platforms and Changing Threats, *Security Threat Report 2013*.
- Squicciarini, A. C., Xu, H. and Zhang, X. (2010). CoPE: Enabling Collaborative Privacy Management in Online Social Networks, *Journal of the American Society for Information Science and Technology*, doi: 10.1002/asi.21473.
- Westermann, D. A. (2011). Mom, dad, let's be (Facebook) friends: exploring parent/child Facebook interaction from a communication privacy management perspective, Unpublished thesis, Kent State University.
- Wisniewski, P., Knijnenburg, B. P., & Lipford, H. R. (2014). Profiling Facebook Users' Privacy Behaviors, *Paper presented at Symposium on Usable Privacy and Security (SOUPS) 2014*, July 9-11, 2014, Menlo Park, CA.
- 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, D. R., Willaert, K. & Pierson, J. (2014). Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior*, 35(2014), 444-454.
- Venkat, A., Pichandy, C., Barclay, F. P., & Jayaseelan, R. (2014). Facebook Privacy Management: An Empirical Study of Awareness, Perception and Fears, *Global Media Journal-Indian Edition*, 5(1) pp. 1-20.