

The copyright © of this thesis belongs to its rightful author and/or other copyright owner. Copies can be accessed and downloaded for non-commercial or learning purposes without any charge and permission. The thesis cannot be reproduced or quoted as a whole without the permission from its rightful owner. No alteration or changes in format is allowed without permission from its rightful owner.



INFORMATION REVELATION AND INTERNET PRIVACY ON  
MOBILE SOCIAL NETWORK SITE (FACEBOOK):  
A CASE OF UNDERGRADUATE STUDENTS IN  
SCHOOL OF BUSINESS MANAGEMENT, UUM

NORHANIL HEKMAH BINTI ROSLI



UUM  
Universiti Utara Malaysia

MASTER OF SCIENCE (MANAGEMENT)  
UNIVERSITI UTARA MALAYSIA  
JUNE 2018

**INFORMATION REVELATION AND INTERNET PRIVACY ON  
MOBILE SOCIAL NETWORK SITE (FACEBOOK):  
A CASE OF UNDERGRADUATE STUDENTS IN SCHOOL OF  
BUSINESS MANAGEMENT, UUM**

**By**

**NORHANIL HEKMAH BINTI ROSLI**



**UUM**  
Universiti Utara Malaysia

Thesis Submitted to  
Othman Yeop Abdullah Graduate School of Business,  
Universiti Utara Malaysia,  
in Partial Fulfillment of the Requirement for the Master of Sciences (Management)



**Pusat Pengajian Pengurusan  
Perniagaan**

SCHOOL OF BUSINESS MANAGEMENT

**Universiti Utara Malaysia**

**PERAKUAN KERJA KERTAS PENYELIDIKAN**  
(*Certification of Research Paper*)

Saya, mengaku bertandatangan, memperakukan bahawa  
(*I, the undersigned, certified that*)

**NORHANIL HEKMAH BINTI ROSLI (818167)**

Calon untuk Ijazah Sarjana  
(*Candidate for the degree of*)

**MASTER OF SCIENCE (MANAGEMENT)**

telah mengemukakan kertas penyelidikan yang bertajuk  
(*has presented his/her research paper of the following title*)

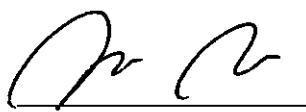
**INFORMATION REVELATION AND INTERNET PRIVACY ON MOBILE SOCIAL NETWORK SITE  
(FACEBOOK): A CASE OF UNDERGRADUATE STUDENTS IN  
SCHOOL OF BUSINESS MANAGEMENT, UUM**

Seperti yang tercatat di muka surat tajuk dan kulit kertas penyelidikan  
(*as it appears on the title page and front cover of the research paper*)

Bahawa kertas penyelidikan tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu  
dengan memuaskan.

(*that the research paper acceptable in the form and content and that a satisfactory knowledge of the field is covered  
by the research paper*).

Nama Penyelia : **DR. ABDUL MANAF BIN BOHARI**  
(*Name of Supervisor*)

Tandatangan :   
(*Signature*)

**DR. ABDUL MANAF BOHARI**  
Head Department of Management and  
Entrepreneurship  
School of Business Management  
College of Business  
Universiti Utara Malaysia  
**10 JANUARI 2018**

Tarikh : **10 JANUARI 2018**  
(*Date*)

## **PERMISSION TO USE**

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree Master of Science (Management) from University Utara Malaysia, I agree that the university's library may it freely available for inspection. I further agree that permission for copying this thesis in any manner, in a whole or in a part, for scholarly purpose may be granted by my supervisor or in their absence, by the Dean of Othman Yeop Abdullah, Graduate School of Business, UUM. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part shall be addressed to:

Dean of Postgraduate  
UUM College of Business  
University Utara Malaysia  
06010 Sintok  
Kedah Darul Aman

## DISCLAIMER

I am responsible of the accuracy of the opinion, technical comment, factual report, data, figures, illustrations and photographs in the article. I bear full responsibility for the checking whether material submitted is subject to copyright or ownership right. UUM does not accept any liability for the accuracy of such comment, report and other technical and factual information and the copyright or ownership right claims.

I certify that the substance of this thesis has not already been submitted for any degree and is not currently being submitted for and other degree or qualification. I certify that any help received in preparing this thesis and all sources used have been acknowledged through this thesis.

Student's Signature:



UUM  
Universiti Utara Malaysia

---

(NAME: NORHANIL HEKMAH BINTI ROSLI)

Matric No: 818167

Date: June 4, 2018

## ABSTRACT

This study was about information revelation and internet privacy on mobile social network focusing on Facebook as a most popular social media network. Data were collected using traditional method of questionnaire from a group of 150 undergraduate students in School of Business Management (SBM), UUM that are registered as Facebook user and having active Facebook account. Relationship between Facebook profile elements revelation (relationship status, birthday, education level, photo sharing, and real name) were tested with some other variable such as log on activity, network size, concern about internet privacy, and profile visibility using Crosstabulation and correlation test. Relationship between Facebook profile elements and demographic variable (age and gender) also tested using correlation test. After test has been done, there are significant relationship between education level revelation with personal network size and frequency of Facebook log in-

*Keywords: Facebook, Internet privacy concerns, information revelation, social network sites.*

**KAJIAN TENTANG PENDEDAHAN INFORMASI DAN PRIVASI INTERNET  
DI APLIKASI MEDIA SOSIAL (FACEBOOK):KAJIAN KES TERHADAP  
PELAJAR SARJANA MUDA DI PUSAT PENGAJIAN PENGURUSAN  
PERNIAGAAN UUM**

**ABSTRAK**

Kajian ini adalah tentang penyataan maklumat dan privasi internet di aplikasi rangkaian sosial mudah alih yang memberi tumpuan kepada Facebook sebagai rangkaian media sosial yang paling popular. Data dikumpul menggunakan kaedah soal selidik dari sekumpulan 150 pelajar sarjana muda dari Pusat Pengajian Pengurusan Perniagaan (SBM), UUM yang berdaftar sebagai pengguna Facebook dan mempunyai akaun Facebook aktif. Hubungan antara elemen profil Facebook yang didedahkan kepada umum (status, hari lahir, tahap pendidikan, perkongsian foto, dan nama sebenar) diuji dengan beberapa pembolehubah lain seperti kekerapan log masuk, saiz rangkaian, kecenderungan mengenai privasi internet, dan pendedahan profil menggunakan Crosstabulation dan ujian korelasi. Hubungan antara elemen profil Facebook dan pembolehubah demografi (umur dan jantina) juga diuji menggunakan ujian korelasi. Setelah ujian telah dilakukan, terdapat hubungan yang signifikan antara pendedahan tahap pendidikan dengan saiz rangkaian dan kekerapan log masuk Facebook.

*Kata kunci : Facebook, keseimbangan privasi Internet, pendedahan maklumat, media sosial*



Universiti Utara Malaysia



## **ACKNOWLEDGEMENT**

Million thanks for an outstanding cooperation by all staff at School of Business Management and Othman Yeop Abdullah Graduate School of Business that have made the creation of the thesis a pleasure. My supervisor, Dr. Abdul Manaf Bohari, enthusiastically support and backed the project and play a large role in completing the thesis. Thank you very much for the invaluable guidance, encouragements, suggestions, comments, and assistances through-out the period of this thesis. User's kind advice will encourage me to do further research in future.

I also want to express thousand thanks to the administration staff of the school for valuable information, supply many insightful reaction, and suggestions for final works improvements especially for Prof. Dr. Haim Hilman Abdullah, Dean of School of Business Management, UUM. Also, I am particularly grateful to my colleagues, friends, and course-mates who in anyway help me through this research paper.

Finally, I am indebted to my husband and my children. Thanks a lot for giving me more chance and more time to complete this final report. Special thanks for their support, commitment, and understanding in helping me pull through this course. I appreciate the contribution from all of my family. All of user are wonderful helpmate. Thank user for everything.

NORHANIL HEKMAH BINTI ROSLI

June 4, 2018

# TABLE OF CONTENT

	<b>PAGE</b>
Permission to use	iii
Disclaimer	iv
Abstract	v
Abstrak	vi
Acknowledgement	vii
Table of Content	viii
List of Figures	xiii
List of Tables	xiv
List of Charts	xv
<b>CHAPTER ONE: INTRODUCTION</b>	
1.1 Introduction	1
1.2 Background of the Study	1
1.3 Problem statement	4
1.4 Research objectives	6
1.5 Research questions	7
1.6 Scope of the study	8
1.7 Significance of study	7
1.8 Summary	8

## CHAPTER TWO: LITERATURE REVIEW

2.1	Introduction	9
2.2	Definition of terms	9
2.2.1	Definition of information revelation	9
2.2.2	Definition of internet privacy	13
2.2.3	Definition of mobile social network	15
2.3	Facebook	16
2.3.1	History	16
2.3.2	Facebook usage frequency	18
2.3.3	Network size in Facebook	19
2.3.4	Concern for internet privacy in Facebook	22
2.3.5	Concern for unwanted audience in Facebook	24
2.3.6	Profile visibility	25
2.4	Mobile social media	25
2.5	Privacy risk in online social network	27
2.6	Awareness of internet privacy	32
2.7	Addiction of mobile social network	33
2.8	Summary	34

## **CHAPTER THREE: RESEARCH METHOD**

3.1	Introduction	35
3.2	Research Framework and Variables Selection	35
3.3	Hypothesis Setting	36
3.4	Research design	37
3.4.1	Questionnaire development	37
3.4.2	Population and sample	38
3.5	Instrumentation	38
3.5.1	Information revelation	39
3.5.2	Frequency of Facebook use	39
3.5.3	Personal Network size	39
3.5.4	Concern for internet privacy	40
3.5.5	Profile visibility	40
3.5.6	Concern for unwanted audience	40
3.6	Procedure of data collection	41
3.7	Summary	41

## **CHAPTER FOUR: RESULTS**

4.1	Introduction	43
4.2	Frequency analysis	43
4.2.1	Respondent status	43
4.2.2	Gender	44
4.2.3	Age	44
4.3	Information revelation on Facebook	45
4.4	Usage	47
4.4.1	Log on activity	47
4.4.2	Facebook friends and connections	48
4.4.3	Internet privacy concern	49
4.4.4	Profile visibility	50
4.5	Results Analysis	51
4.5.1	Facebook log on activity and information revelation	51
4.5.2	Personal network size and information revelation	52
4.5.3	Concern for internet privacy and information revelation	53
4.5.4	Profile visibility and information revelation	54
4.5.5	Concern for unwanted audiences and information revelation	55
4.6	Correlation test	56
4.4.1	Gender and information revelation	56
4.4.2	Log on activity and information revelation	58

4.6	Conclusion	59
-----	------------	----

## **CHAPTER FIVE: DISCUSSION AND CONCLUSION**

5.1	Introduction	60
5.2	Discussion of findings	
5.2.1	Facebook log on activity and information revelation	60
5.2.2	Facebook personal network size and information revelation	60
5.2.3	Concern for internet privacy and information revelation	61
5.2.4	Profile visibility and information revelation	63
5.2.5	Concern for unwanted audiences and information revelation	63
5.3	Suggestion related to mobile Facebook privacy	64
5.4	Future research recommendation	66
5.5	Limitation	67
5.6	Conclusion	67

## **REFERENCES**

## **APPENDICES**

## LIST OF FIGURE

## PAGES

Figure 1	Percentage of personal network size in Facebook	21
Figure 2	Theoretical framework	36



**LIST OF TABLES****PAGES****Table**

Table 1	Respondent account in Facebook	43
Table 2	Frequency of Gender	44
Table 3	Frequency of Age	44
Table 4	Statistic of Facebook log on activity	47
Table 5	Personal Facebook network size	48
Table 6	User internet privacy concern in Facebook	49
Table 7	User's profile visibility	50
Table 8	Facebook log on activity and information revelation	52
Table 9	Personal network size and information revelation	52
Table 10	Internet privacy concern and education level revelation	53
Table 11	Profile visibility and information revelation	54
Table 12	Unwanted audiences and information revelation	55
Table 13	Correlation for gender and status	56
Table 14	Frequency of status and gender	57
Table 15	Log on activity and information revelation	58
Table 16	Log on activity and information revelation	58



## LIST OF CHART

## PAGES

### Bar Chart

Bar Chart 1	Information revelation based on Facebook profile elements	6
Bar Chart 2	Log on activity	47
Bar Chart 3	Personal network size	48
Bar Chart 4	User internet privacy concern	49
Bar Chart 5	Frequency of Facebook profile visibility	50



# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 Introduction**

This chapter will discuss the introduction of information revelation, internet privacy, and mobile social network in general as a background of this research. It will also explain the problem statement by taking into account the previous study to find out why this problem occurs and to state the objective of the study with the issue of relationship between information revelation on Facebook and frequency of Facebook log on activity, personal network size, concern for internet privacy, profile visibility, and concern for unwanted audiences. Last but not least, authors will brief the significance of this research implemented and this chapter will be wrapped up with the summary of the chapter.

### **1.2 Background of the Study**

Sharing of personal information in the virtual world is not too bad if it does not negatively impact the user. In fact, it makes it easier for other virtual world users to track the characteristics of individuals who have similarities with them to communicate with each other in a positive way. It becomes a concern if the publicly disclosed information is used by a particular party with bad purpose and affects the user. Saieed, (2017) through The Star Newspaper reported fraud cases detected in cyberspace jumped 20% last two years compared to 2015 also 2,428 cybercrime incidences reported between January and April of 2017; estimated will be increasingly challenging due to the exponential growth of

connected devices. In this study, we narrow the topic and focus to information revelation in Facebook and set the goal to find which part of the profile respondent like to reveal.

Facebook has been so famous since its launch by Mark Zuckerberg in 2004. Since it was a user-friendly website, it gives the user the freedom to input information based on the type of information requested. The user is free to set the audience that is allowed to view the information in the user profile. Information revelation, internet privacy, and mobile social network were being the main three pillars to start this study since the goal was to investigate the reason of information revelation in Facebook.

Facebook offer attractive means for interaction and communication, but also raise privacy and security concerns (Acquisti, 2009) where the websites allow people to create their profiles and share this information with their friends and a vast amount of strangers on these social sites (Mushtaq, 2008). Nobody is really forced to join social network site (Taraszow, Aristodemou, Shitta, Laouris, & Arsoy, 2010), create a profile and reveal personal information as their self-presentation (Tufekci, 2008), but in order to join social media network, they are compulsory to fill in the form about basic personal information such as name, date of birth, gender, mobile number, email address and uploading photo.

Many social network sites offer an option to the user to choose their profile to be visible by public, friends and acquaintance, or friends only. User also can block other user from seeing his/her updates on wall or private message. Starting from 2008, after complaints the company received regarding violations of people's privacy rights, Facebook profiles by default visible to friends only, with the option to change one's own profile into a public

one (Taraszow, Aristodemou, Shitta, Laouris, & Arsoy, 2010). This was the thing that is most fascinating about Facebook on how it illuminates the changing nature of public and private identity (Hodge, 2007). In borderless world, everything can be spread in a blink. As an example when somebody uploading a video of police smoking in their uniform, friends of the user that upload the video can share the video to his/her friends list, and friends of friends continuingly can share the video until its being viral. End up with the person in the video can be subject to disciplinary action or even worse, fired.

Recent years have witnessed the rapid proliferation and widespread adoption of a new class of information technologies (Kane, Alavi, Labianca, & Borgatti, 2012) so called as social media network that entitled to introducing new features and attracting different user demographics background. It has attracted millions of users such as MySpace, Facebook, Cyworld, and Bebo who integrated these sites into their daily practices (Boyd & Ellison, 2007) and do create, modify, share, and discuss internet content among acquaintances (Kietzmann, McCarthy, Hermkens, & Silvestre, 2011). Normally, users profile contains an array of information about the user, describing himself with elements such as physical appearance, hobbies, personal photo and/or pictures of friends, contact information and a vast array of other user contributed content (Mushtaq, 2008).

According to market research company Gartner, there could be 20.4 billion Internet of Things (IoT) connected devices between now and 2020 (Saieed, 2017). At the same time, the development of mobile applications designed to increase efficiency and productivity for professionals on the go (Smith & Holmes, 2005) but people install and

use such mobile applications to satisfy their growing needs as well to connect and communicate with others (Salehan & Negahban, 2013) and dangerously can be an addiction to social media network if used frequent time.

### **1.3 Problem Statement**

As the most popular social media network where a millions people download in apps, Privacy International charged Facebook with severe privacy flaws and put it in the second lowest category for substantial and comprehensive privacy threats which are very dangerous to reveal personal information that can be access public all around the world that having internet access. There are a number of security issues putting user in a serious risk if they are compromise with their personal information. User's identity can be hacked easily by anonymous since it was so easy to run malicious program using any application that being a favorite of the community such as quizzes regarding fate forecast and zodiac.

Although mobile phones are very popular and inseparable part of our lives (Li, Cao, & Yu, 2011), various social issues have arisen during their adoption, including use of mobile phones in banned and dangerous circumstances (Bianchi & Phillips, 2005). Disclosing personal information on social network users effectively place themselves at a greater risk for cyber and physical stalking, identity theft and surveillance (Gross & Acquisti, 2005). Data brokers who hold information about things such as people's personal Web browsing habits will be especially popular targets.

Users publish their dates of birth, hometowns, current residences, home and cell phone numbers, or sexual and political preferences, with little control on whom may access those data (Acquisti, 2009) where they experimenting with new ways of networking and socializing without any concern the risk any people will manipulate their data and putting them at risk of current or future identity theft, online and physical stalking, or blackmailing. This action (information revelation via social media) was trusted to be influence by future audiences, gender, and general privacy concerns. Tufekci (2008) in his study list down three important factors influence information revelation including future audiences, gender, and general privacy concerns.

The amount of user-generated media uploaded to the web is expanding rapidly and it is beyond the capabilities of any human to sift through it all to see which media impacts their privacy (Smith, Szongott, & Henne, 2012) and unfortunately there is still no end to this trend in sight. The ease-of-use of modern smartphones and the proliferation of high-speed mobile networks are facilitating a culture of spontaneous and carefree uploading of user-generated content. To give an idea of the scale of this phenomenon, Just in the last two years (on 2008) the number of photos uploaded to Facebook per month has risen from 2 billion to over 6 billion (Eldon, 2010).

Current social networks sites mainly focus on the privacy of users' own media in terms of access control, but less privacy implications created by other users' media. Settings allowing a user to decide who is allowed to see what content but only for the media content owned by the user but not for the issue of staying on top of what others are uploading that

might be relevant to the user, was still very much outside the control of that user. Research supporting a privacy paradox among adolescent's shows that only a minority of using social media users changed the default privacy settings from public to private (Velven & Emam, 2013) and that there seems to be a discrepancy between stated privacy concerns and the disclosure of private information.

Users are generally unaware of who has access to their private information (Krishnamurthy & Wills, 2008) yet Facebook gives users no choice if they want to download and use an externally created application. Although sites offer privacy controls that let users restrict how their data is viewed by other users, sites provide insufficient controls to restrict data sharing with corporate affiliates or application developers (Randy Baden, 2009). Not only are there few controls to limit information disclosure, acceptable use policies require both that users provide accurate information and that users grant the provider the right to sell that information to others.

#### **1.4 Research Objectives**

This study had four objectives as below:

- to investigate Facebook usage and profile elements
- to examine Facebook network size and information revelation
- to investigate concern for internet privacy and information revelation.
- to examine relationship between concern for unwanted audience and information revelation

### **1.5 Research Questions**

The main issue for this study was the relationship between information revelation on Facebook and frequency of Facebook log on activity, personal network size, concern for internet privacy, profile visibility, and concern for unwanted audiences. This research tried to investigate and solve the following research questions:

1. Is there any relationship between Facebook usage and profile elements
2. Is there any relationship between Facebook network size and information revelation
3. Is there any relationship between concern for internet privacy and information revelation.
4. Is there any relationship between concern for unwanted audience and information revelation?

### **1.6 Scope of the study**

This research was done in Universiti Utara Malaysia in 2017 (semester A171) where the respondents were from School of Business Management, UUM which having personal Facebook account. Information revelation elements in Facebook were analyzed to know its relationship between frequency of Facebook log on activity, concern for internet privacy, concern for unwanted audiences, profile visibility and Facebook personal network size.



## **1.7 Significance of the study**

Many found that Facebook is deeply integrated in users' daily lives through specific routines and rituals (Debatin, Lovejoy, M.A., & Hughes, 2009). On the awareness of this issue, this research was created to help users to be more sensitive and careful in choosing personal information disclosed on social sites and tightening security and friend access to profiles.

The contributions of this study would be of interest to scholars in information technology as well as to practicing managers, particularly in data entry industry. Besides, I am taking personal responsibility for online privacy and security as the most important ingredient in stemming the tide of cybercrime, there is also a role for government and law enforcement. We as individuals need to demonstrate that privacy and security in the digital realm is a top priority that we are willing to take collective responsibility to protect ourselves from growing threats to our online privacy and freedom (Gorodyansky, 2017).

## **1.8 Summary**

In this chapter, we can conclude that information revelation, internet privacy, and mobile social network were the main point to further this research to the next chapter. Relationship between frequency of Facebook log in, Facebook personal network size, and internet privacy concern will be test in chapter 4 whether it were related to the information revelation on their Facebook profile. Next chapter will discuss regarding literature of information revelation, internet privacy and mobile social network; also some point related to Facebook.

## **CHAPTER 2**

### **LITERATURE REVIEW**

#### **2.1 Introduction**

This chapter will discuss about the definition of information revelation, internet privacy, mobile social network and introduction of Facebook in general. It will also discuss about the revolution from social media to mobile social media among teenagers. Finally, the wrap will be a previous study regarding risk of information revelation, awareness of internet privacy, and addictive of mobile social network.

#### **2.2 Definition of terms**

Until today, it is not well understood how privacy concern and trust can be put on easily on social networking sites. In order to find the answer, this part will explain regarding definition and key elements of each main pillars in this study.

##### **2.2.1 Definition of information revelation**

With the growing popularity of online social networks, more and more personal information is being displayed on websites. This is despite the fact that privacy groups advise Internet users not to “reveal personal details to strangers or ‘just-met friends” (McCandlish 2002). Privacy groups cite social consequences of risky online behavior as harassment, stalking, and spamming (“Privacy in Cyberspace” 2005). While Internet users may feel safe behind their computers, they have “zero privacy” (Regan 2003).

At the same time, others may have published information about user. Friends (or ex-friends) may write about user or post photos of user and family. Interest groups, clubs, and professional associations may reveal user's full name, workplace or school and other details without any permission or request.

This information is often permanent and searchable, especially if the privacy settings of individual social accounts are set to "public". In such an instance, a simple search could easily help someone piece together a composite profile of user. Predators may use the information to get close to user. Criminals may use the data to target user for scams or steal identity to commit other crimes.

Organisations are also collecting information about user as they surf the web, download software, make purchases, register for a contest, or take part in a survey. They may track and collect information indicating user's shopping preferences, habits and interests. These organisations may then use such data (which could identify user as an individual) for various other purposes such as customer profiling, marketing, business analytics or even to sell to other organisations and businesses as part of "database" sales.

As technology becomes increasingly sophisticated enabling the collection and processing of vast amount of personal data, questions arise as to how that data is being used, processed and protected by organisations that collect or possess them. A data protection regime is therefore necessary to address growing concerns of potential

misuse of personal data and maintain trust between individuals and organisations that need to collect and use personal data for legitimate purposes (Media Literacy Council, 2018).

Because there's a part of people tend to live out a good portion of their life on the World Wide Web, it's easy to forget that having a life online also means that countless numbers of people have access to their personal information at any given time. Whether they are writing a blog post or posting an update on Facebook, it's easy to overlook breaches to individual's electronic privacy. As prying eyes are able to access personal data in various ways, it's critical that user constantly work to keep their personal information private.

Govani & Pashley, (2005) on their study have found that most students are aware of possible consequences of providing personally identifiable information to an entire university population, such as identity theft and stalking, but nevertheless feel comfortable providing it. Despite the overwhelming majority of survey participants knowing that they are able to limit who views their personal information, participants did not take the initiative to protect their information.

Every time people join a social network, fill in a profile, blog, share a video, send a tweet, or post a comment, they create a digital footprint that is both permanent and potentially public. What they say and share give people an idea of what they are like as a person.

In social network site, users want to be seen by others, with the intention of contacting or being contacted by others (Gross & Acquisti, 2005) so they can build a networking and communicate each other rather than keep their profile on private mode. To be seen, they had to make themselves stand out by make everyone knows about themselves and from the similarity of the features, acquaintances attracted to make them friends other than known friends in the real world. For instance, user may reveal their location, so the people around that location will attracted to know them; and its going to be easier if the user also reveal their age, contact number or email so the friendship can be continued in the real world using the reason because of user live in the same location or nearby.

The doubt was not all the people in social network site are good people. They might having hidden agenda than may harm others or they was a criminal person that intend to do bad things like raping and robbing. Or else, somebody may use the same personal information to do criminal somewhere using fake account and the effect are of course will tarnish the image owner of the personal information. Golijan, (2012) in her consumer report says personal data is shared more widely than user may wish. Even if they have restricted the information to be seen by friends only, a friend who is using a Facebook app could allow the data to be transferred to a third party without knowledge of the original owner; which is the data might be manipulated, edited or changed without permission.

### **2.2.2 Definition of internet privacy**

“Privacy” has become a powerful keyword, a shorthand tag that gets used to reference a constellation of public attitudes, technical affordances and legal arguments. Yet, the concept is so laden with multiple meanings that any use of the term begs for added specificity and context (Madden, 2013). The first concept focuses on the full protection of any individual, which according to Warren and Brandeis (1890) includes ‘the right to privacy’, where privacy is understood as the ‘right to be let alone’ (Warren and Brandeis 1890). Although consumers report that they are concerned about privacy issues (Stark and Hodge 2004) but social network encourage their users to reveal and exchange personal information are booming in popularity.

Madden, (2013) report that the complexity of privacy settings varies greatly across different social media sites, and in the case of Facebook, the default settings have changed significantly over time. In all, 48% of social media users report some level of difficulty in managing the privacy controls on their profile, while 49% say that it is “not difficult at all.” Few users (2%) describe their experiences as “very difficult,” while 16% say they are “somewhat difficult” and another 30% say the controls are “not too difficult” to manage. Adults are considerably more likely than any other age group to feel fully confident in their privacy controls; 57% of social media users ages 18-29 say it is “not difficult at all” to manage them, compared with 48% of those ages 30-49, 41% of those ages 50-64 and 31% of those ages 65 and older.

The internet was such an amazing tools that can find almost anything in the world as long as long as its connection available. It also allows for the efficient and inexpensive collection of vast amounts of information (Chung, 2002) and the types of information were totally controlled by the user. Since that internet was international and largely unregulated, the laws of any one country do not usually apply to internet activities originating in other countries. The internet has a vast potential for privacy violation as technological innovations have become more advanced (Zimmerman, 2001) now days.

Strategic uses of information technology based on personal information may raise privacy concerns among users if these applications do not reflect a common set of values. Privacy defines as right to be alone (Warren & Brandeis, 1890) and invasions of privacy usually occur when individuals cannot maintain a substantial degree of control over their personal information and its usage (Lim, 2000). Information privacy exists when the usage, release and circulation of personal information can be controlled (Culnan, 1993).

Privacy concerns are identified as one of the main factors that have a negative impact on Internet users' online behavior (Mekovec & Vrcek, 2011) since many Internet users do not seem to value privacy much (Miller, 1997) although research they know that individuals with profiles on social networking websites have greater risk taking attitudes than those who do not (Fogel & Nehmad, 2009). The monetary value of this information explains why so many websites gather personal information (Chung,

2002) when data entered into forms or contained in existing databases can be combined almost effortlessly with transaction records and records of an individual's every mouse-click.

### **2.2.3 Definition of mobile social network**

With the evolution of the mobile platform and the rapid adoption of mobile devices such as cell phones and other handheld devices, social networks, which began as Web-based applications, have migrated onto the mobile platform (Ziv & Mulloth, 2006). Mobile social networks are the impetus for the creation of an entirely new sub-industry in the wireless sector, thus representing a new aspect of wireless innovation, and increasingly are providing a platform for content and technological innovation in the business environment.

Mobile social network is a typical social network where one or more individuals of similar interests or commonalities, conversing and connecting with one another using the mobile phone (Dong, Song, Xie, & Wang, 2009). When it's become broader worldwide, the privacy implications associated with this class of software, suggesting that broad adoption may only happen to the extent that these concerns are adequately addressed (Sadeh, 2008). While online communities were initially only accessible through websites and therefore one-dimensional from a technological point of view, with the development of the mobile platform, hybrid online/mobile communities have emerged with users participating both through a website and by using their mobile devices.



According to the reports by Mei-Pochtler,(2017) increasing pattern of mobile internet user were happened year by year. Current year (2017) record 19.06 million active mobile internet user in Malaysia and the value estimated to be increase for the following year. People being comfortable using mobile social network since it meets the needs of the user and simplifies access on the account anywhere as long as the internet connection was available around. The features of android ( easy to carry as small android sizes) add more advantages of using mobile phone to surfing social network. Facebook's user friendly application grants users free mobile access to certain websites, is likely to have driven some of the growth in mobile use of the platform (e-Marketer, 2016). The application was free and can be downloaded without any problem.

## **2.3 Facebook**

### **2.3.1 History**

Facebook begin 13 years ago on 2004 as an American for-profit company providing social networking services from the headquarters located in Mento Park, Callifornia, United States. It was manage by a group of executives (also founders of Facebook) including Mark Zukerberg, Sheryl Sandberg, David Wehner, Mike Schroepfer and Chirs Cox.

Facebook was the most popular social media network that offered free membership and allows registered users to create profiles, send messages, upload photos and video and keep in touch with friends and aquanitances via homepage address

<http://www.facebook.com>. From the email or phone number that registered by the user, Facebook log on activity the contact from the email to identify the list of friends and nearby people known by users and gives them the option to add that person as a friend so they can connect as a friend via Facebook; also can share, like and comments status written by their friendlist. As an option, Facebook available in more than 20 international languages to making it easier for users to communicate.

For the first step to register as a user, Facebook only ask for first name, surname, mobile number or email address, password, birthday, and gender to create an account (refer Figure 2). If the user was public figure, they were recommended to create a page instead of personal account. Second step was uploading a status containing a sentences with photo or video. User also can also go live, mention their specific location, creating a poll, includes the emoticon or sticker of their feelings and activities. They also allowed to tag their friends on the status, change the background color of the status, do slideshow of their own photo, also ask for recommendations about certain places.

Facebook also offered to the user the audience who can see the post as below :

- a) Public - anyone including anonymous can access the status
- b) Friends only – only the person on their friendlist can see the post
- c) Friend except - all friend in the friendlist can read the post except spesific person
- d) Spesific friends – only the friends selected can see the post
- e) Only me – only user can see the post

User had an authority to edit or delete the post if they want at anytime. Person tag on their friend post also can set who can view the post that they have been tagged. On the comments section, anyone on the allowed list can reply on the spesific comments, edit or delete it.

### **2.3.2 Facebook usage frequency**

70% of smartphone users are frequent Facebook visitors, with more than half of them checking it every day. Peak Facebook time is during the evening, just before bed. But any time's good: on average, we visit the Facebook app or the site 13.8 times during the day, for two minutes and 22 seconds each time (Taylor C. , 2013). About half of that daily half-hour on the social network, user simply browsing their News Feed. The rest of the time is divided fairly evenly between Facebook messaging and posting updates or playing games in the Facebook.

Smith K. , (2018) in his article code that there are 1.37 billion daily active user log on to the Facebook where over 1 billion are mobile-only users with an addition of 6 new Facebook profile every second. From that statistic, over 81 millions are fake account that made by consumers to sign into the apps and websites of publishers and brands – also from the stalker. Previous research by Michel Ballings, (2015) was true when statista.com reports of the increasing pattern of registered Facebook account in Malaysia year by year as below where for the current year, there were 11.9 million active Facebook account. According to Malaysian Communications and Multimedia

Commission (MCMC) report regarding internet user in 2016, 80% Malaysian spending their time using internet to enjoy social media network while 96.5 of the respondent that roughly test were having Facebook account with the mean age of 32 years old with average 4 hours per day time spending on social media site (MCMC, 2016).

Statista, (2018) has report 62% of the respondents on their study will log in to Facebook once a day while Taylor C. ,( 2013) writes 70% of smartphone users are frequent Facebook visitors, with more than half of them checking it every day with the average of 14 times log in per day. Normally, about half of that daily half-hour on the social network, users were simply browsing their News Feed. The rest of the time is divided fairly evenly between Facebook messaging and posting updates. Half of Facebook users play games via the service on their phone a few times a day. Leonard, (2013) state on his article in Business Insider that user spend at least 55 minutes per day to send 2 friend request, click the likes button 9 times, being a member of 5 group, writes 25 comments, and become fan of 2 pages.

### **2.3.3 Network size in Facebook**

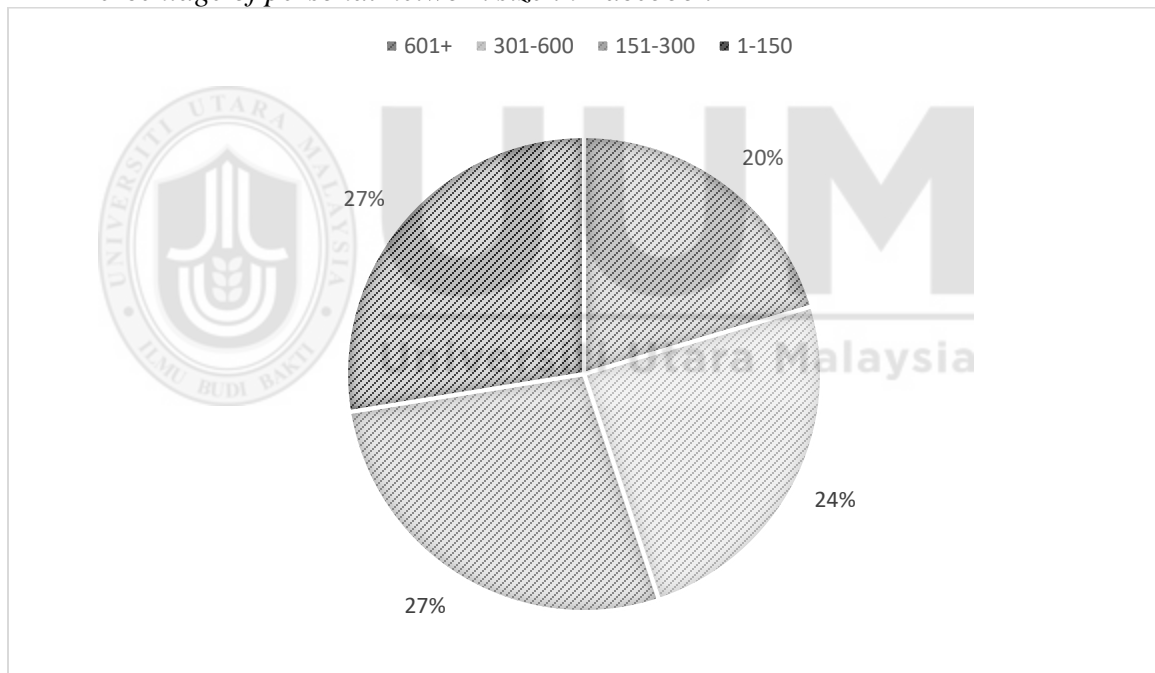
Walther, et al., (2008) hypothesize individuals with too many friends may appear to be focusing too much on Facebook, friending out of desperation rather than popularity, spending a great deal of time on their computers ostensibly trying to make connections in a computer-mediated environment where they feel more comfortable than in face-to-face social interaction

Every person can have a maximum of 5,000 connections on Facebook, which include both friends and pages. User will not be able to accept incoming friend requests or like any more pages if they get to that number (Graham, 2012). If user have too few "friends" on Facebook, people might think user are a loser. Too many and people might think user are a social slut. According to Lin & Qiu, (2012) person's network size usually increases over time with new friends being added and friendships being extended. From a study by Hampton, Sessions, & Her, (2010), mobile phone and Internet use, especially specific uses of social media, having a positive relationship to network size and diversity. They also speculate that specific social media provide for a 'pervasive awareness' within personal networks that has increased the specialization of close ties. Normally, Facebook account for business will having friends until maximum to make it easy to connect with the potential customer and make them loyal to buy.

According to Sarah Knapton (2016) in her online article, collecting hundreds of Facebook friends may seem like a sure-fire way to boost popularity but a new study suggests that fewer than three per cent can be relied on in a crisis. In addition, researchers found that the average Facebook user has 155 friends (women averaging more than men) but would turn to just four for help and 28 per cent to be genuine, or close, friends and said they would turn to just four in a crisis.

Figure 1 below shows percentage of network size of teenagers by Madden, ( 2013). According to the report, user sharing more information about themselves on social media sites than they did in the past with 300 median number of Facebook friends. Madden also conclude increasing network size goes hand in hand with network variety, information sharing, and personal information management with girls and older teens tend to have substantially larger Facebook friend networks compared with boys and usernger teens where largely mirror their offline networks

Figure 1  
*Percentage of personal network size in Facebook*



Source: Madden, (2013)

From a random interview to the respondent involve, he has 400 friend in his account and normally interact with 150-200 of them. The others are acquaintances, people who don't use Facebook much, people he used to know, or in a few cases just people who sent him friend requests and seemed not particularly obnoxious.

Facebook lets friends connect. They can give each other updates, share photos and post comments. But that's not all. Facebook might also stress users out. Perhaps managing huge numbers of Facebook friends just takes too much work. Or, maybe most of them are mere acquaintances instead of close, supportive friends (Kowalski, 2015).

#### **2.3.4 Concern for internet privacy in Facebook**

Almost every time Facebook rolled out a major new feature, it made member information more accessible, rather than less (Tan, 2012). Facebook's ever changing privacy policy and privacy control during a speech, Facebook founder Mark Zuckerberg said, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time" (Johnson B. , 2010).

Teens share a wide range of information about themselves on social media sites; indeed the sites themselves are designed to encourage the sharing of information and the expansion of networks (Madden, 2013). Among teen Facebook log on activities, most choose private settings that allow only approved friends to view the content that they post especially girls. Madden (2013) again reports more than half (56%) of teen Facebook log on activities say it's "not difficult at all" to manage the privacy controls on their Facebook profile, while one in three (33%) say it's "not too difficult." Just 8% of teen Facebook log on activities say that managing their privacy controls is "somewhat difficult," while less than 1% describe the process as "very difficult."

Based on general privacy settings, teen Facebook log on activities have the option to choose a limit on who can see the information and updates they post crawling on their daily newsfeed. However, few choose to customize in that way: among teenagers Facebook log on activity, only 18% say they limit what specific friends can see on their profile. The vast majority (81%) say that all of their friends can see all things on their profile without any filter. This approach also extends to parents where only 5% of teen Facebook log on activity say they limit what their parents can see.

Cecere, (2015) in her study had observe both cultural and socio-demographic variables affect the level of privacy concerns. While Houghton, (2017) found that consumers appear to trust social network site to protect their private information, they are reluctant to trust advertising or brands on these sites and felt their social life was more important than their privacy concerns.

Social media rely on user bases giving it data. They deal in data, communicate using our data, analyze markets using that data, and build their business models on the back of all the personal data we provide to it that represent digital self of user that can be use by company to tailor their view of user and supposed needs.

Rosenblum, (2007) code the posting of personal and private information in social media opens up a user to public scrutiny, possibly creating permanent records that can affect the user negatively in the future and agreed by Boyd, (2008) by state that personal information reveals online far more accessible and visible, posing a disruption of privacy also despite some anecdotal evidence.



### **2.3.5 Concern for unwanted audiences in Facebook**

The unintended audience is the new norm. And with it, we have burdened ourselves with the worry of not knowing where our communications might surface. Facebook user share information with others by creating posts and specifying who should be able to see each post. Once a user creates a post, those who see it have the ability to copy and re-share the information. But, if the reader has a different understanding of the information in the post than the creator intended, he or she may use the information in ways that are contrary to the intentions of the original creator (Jung & Rader, 2016). User might unintentionally allow the information to be disclosed to someone that she does not intend to receive it by mis-managing privacy settings or being unaware of who has the ability to see her posts and the user's Facebook friends who see the post could re-share that information with others against the user's wishes.

Privacy was an attribute an individual could choose. It made life easier. It was not something we planned to give up as citizens swept up into the digital world. Based on the study by Jung & Rader (2016), they found that user had similar levels of privacy concern about a post shared with an imagined audience of friends and friends of friends. However, reader believed posts were more private than the user themselves did, and showed more privacy concern.

### **2.3.6 Profile visibility**

Public information was something that's public can be seen by anyone. That includes people who aren't user's friends, people off of Facebook and people who use different media such as print, broadcast and other sites on the Internet. For example, if user uses Facebook services to provide a real-time public comment to a television show, that may appear on the show or elsewhere on Facebook. According to Facebook Help (Facebook, 2017) anyone can see user's public information, which includes name, profile picture, cover photo, gender, username, user ID (account number), and networks. When users choose to share something with Public, it's considered public information. If they share something and don't see an audience selector or another privacy setting, that information is also public or else, they can choose audience in audience selector setting.

## **2.4 Mobile social Media**

Almost all of generation Y (people who born between 1981 until 1999) rely heavily on technology for entertainment, to interact with others also for emotion regulation (Ruth N. Bolton, 2013). As more and more Facebook usage moves from the desktop to the mobile version of the site, user behavior is changing. Pew Internet reports have noted that internet connectivity is increasingly moving off the desktop and into the mobile and wireless environment, particularly for specific demographic groups (Horrigan, 2009). Facebook statistics on March 2009 state there are currently over 30 million active mobile users of Facebook (Aaron Beach, 2009), and those users are almost 50% more active on Facebook than non-mobile users. According to the invention by Finucan, (2009), users manage local

profiles on their wireless devices which form ad-hoc networks with any other devices they encounter, exchange profile data to establish a degree of commonality or interests, and may meet during their normal daily lives.

A study of Lenhart et. al (2010) noted that average of teenagers nowadays owned their cellphone as early as twelve and they are doing daily communications with friends via social media besides of getting news about current events. This situation making them comprised of 81% wireless internet users compared to desktop where two third of them go online every day. According to a poll by Common Sense Media, 22% of teenagers log on to their favorite social media site more than 10 times a day, and more than half of adolescents log on to a social media site more than once a day (Common Sense Media, 2009). Since Facebook was an online application, it was allowing information about users' preferences and social relationships to interact in real-time with their physical environment (Aaron Beach, 2009) without prioritizing privacy issues and the possibility of users being exposed to dangers by strangers.

Facebook Mobile is a feature that allows a user to access Facebook from their cell phone through text messages, e-mails, downloaded applications or a web browser. Launched in 2007, Facebook Mobile was designed to give Facebook users the ability to view and update their pages on-the-go (Rouse, 2010). Status updates, wall posts, and photo uploads can all be done through text and picture messaging, while logging on to the Mobile web site from user's phone's web browser allows user to see friends' updates. Many smart phones also allow a user to download a Facebook application, which comes equipped with many of the the same features available on the standard web site.

In May 2010, Facebook launched "Facebook Zero," a mobile web site which would acquire no data fees, on over 50 service providers around the world. The Facebook app's home page puts links to all of the web site's features on one small, convenient screen. News Feed, Profile, Friends, Messages, Places, and more can be accessed from here, and notifications are shown at the bottom of the screen. If anyone has tagged in a post or photo or written on wall, user will find out about it here (Hall Geisler, 2018). The app also show user a detailed view of information user have shared with other apps and web sites so user can control what these companies have access to.

Facebook also allows user to access any other app that supports Single Sign-On technology. Once user have signed into the Facebook app, user don't have to sign in again to use another Single Sign-On app, like Groupon or Yelp. The idea is to save user the frustration of typing in complicated passwords using tiny keys or on-screen keyboards.

## **2.5 Privacy risk in online social network**

It was quite important to know and understand the privacy risks involved since hacker's prowl the social media networks looking for victims (Cohen, 2016). They usually using shortened URLs to trick their victims visit harmful sites or to inject viruses into their computers or mobile phones via unknown links that will be sent to the victims to their email or private message. Hackers also can easily install spyware remotely via downloads, emails, shortened URLs or instant messages that gives the hacker information about the passwords user use on user's social media networks and other accounts which user access online.

Information available to the public in social media site might be a nightmare to the user. This information is exposed to identity thieves that tend to hack their victim's email accounts by simply using the personal information available on social media profile. For instance, one of the common techniques used is clicking on the "forgot password," and then trying to recover the password via email. Once they access victim's email account, they basically have access to all the personal information (Cohen, 2016).

Access to mobile apps and the location-based services in social media allows users to check in at their current locations. Sharing current location publicly in the social media may be something to be proud of, but it's more like getting likes and comments from all of the people they are connected to their particular social media networks. But the risk of such acts will make the user vulnerable to malicious people who are keen to track their whereabouts or inviting burglars and thieves to the home or business.

Below are why do we need to practice privacy control (Reputation Defender, 2016):

1. Prevent identity theft.

Identity theft is currently the number-one rated cybercrime, and as the Web grows, so will the number of individuals whose identities are stolen online. Identity theft occurs when someone gains access to user's personal information and pretends to be user online. Individuals who have accessed user's personal data can retrieve user's login information for various websites or commit cybercrimes such as fraud, all while posing as user. Identity

theft is the type of crime that can have long-lasting repercussions for both user's electronic privacy and user's online reputation.

## 2. Protect user's banking information.

Many people feel completely safe when banking online, but protecting user's banking information has never been more important. Cybercriminals can take user's banking information and make unauthorized withdrawals and transfers. Although banking websites are encrypted, user should still practice privacy protection by changing user's passwords frequently and by never logging in unless user were on user's protected network at home.

## 3. Avoid posting vacation details.

User may not be the only one excited that user were posting a status update about user's upcoming trip. Unless user's Facebook status updates are completely protected, user may literally be leaving user's front door open to break-ins and home robberies. Never share user's vacation plans on social networking websites.

## 4. Protect user's employment record.

Status updates aren't just for talking to user's friends and followers; they can also give a future employer a quick gauge as to what type of employee user might be like. Sharing personal information such as user's likes and dislikes about politics, religion or user's current job can shut the door on future job opportunities. Be aware of what user were posting on Facebook and Twitter, and ensure a spotless record before user get the job.

#### 5. Manage user's business online reputation.

If user run a business online, user know that practicing business reputation management is something user must do on a daily basis. Failure to protect user's company's electronic privacy can destroy user's online reputation. Criminals can take user's business information and create false email accounts and fake employee names and even hack into user's corporate computer system. Protect user's company's digital privacy by running user's intranet on a secure server.

#### 6. Secure user's credit card information.

Credit card scams are on the rise. Although improvements to SSL technology have allowed user to feel more secure using user's cards online, it's still a good idea to safeguard user's credit card number and security PIN. In addition, user can protect user'sself by asking the credit card company to add extra security questions to user's account and alerts to user's credit bureaus.

#### 7. Gain admission to the school of user's choice.

In much the same way that user's social network status updates and tweets can prevent user from gaining a new job, they can also damage any chances user or user's loved ones have of gaining admission to college. Recruiters and admissions clerks search for applicants online, often judging them solely on their Facebook profile. Check out this article about how Facebook has become the judge and jury of user's online reputation. Keep user's personal information private.

#### 8. Protect user's insurance.

Having proper home insurance is often a necessity for obtaining a mortgage. Like home insurance, life insurance gives user peace of mind that user's family will be protected. If user post personal information on the World Wide Web about risky behaviors involving user or user's home, user could be denied user's insurance plan. Always protect user's privacy by avoiding status updates detailing behaviors that user's insurance company might deem perilous.

#### 9. Defend user in legal proceedings.

Being involved in a lawsuit is stressful, but if user were leaking personal data on the Web user could damage user's ability to win user's case. Never share any type of legal information or post specific details about any type of legal dealings. User may be underestimating those who search for user online.

#### 10. Guard user's medical information.

Posting user's personal information on the Web can prevent user from receiving adequate medical care. Criminals troll websites specifically looking for detailed medical information. When they have obtained user's personal data, they will use it to gain personal medical attention for themselves or to sell to others. User could possibly be denied medical attention due to unpaid debt. Always protect user's electronic privacy by not posting any medical-related data, including information about specific medical conditions.



When user were sitting in front of user's computer at home, it's easy to feel safe while surfing the Internet. Focusing on privacy protection is vital in protecting user's personal data both online and off. So, keep user's personal information private.

## **2.6 Awareness of internet privacy**

Privacy is often thought of as a moral right or a legal right. But it's often more useful to perceive privacy as the interest that individuals have in sustaining a personal space, free from interference by other people and organizations (Clarke, 1999). According to Tamara Dinev (2004) social awareness positively related to the internet privacy concerns since during the explosive development and growth of information technology causing copious amount of personal information has been shared with third parties. Internet users which are socially engaged and have greater social awareness, will tend to know more about the privacy debate, privacy policies, privacy risks associated with Internet, legal implications of privacy invasions and identity thefts (Tamara Dinev, 2004). An important implication of the definition of privacy as an interest is that privacy has to be balanced against many other, often competing, interests, of the individuals themselves, of other individuals, of groups, and of society as a whole.

The greater citizenship engagement and social awareness of an individual, the greater importance that individual would place on privacy as a societal value. According to survey by Govani & Pashley, (2005), students were aware of possible consequences of providing personally identifiable information to an entire online world offered by the social media but they nevertheless feel comfortable providing it. Although they can limit who views

their personal information, participants did not take the initiative to protect their information.

## **2.7 Addiction of mobile social network**

The use of telephones as a communication tool is no longer just by calls and short messages. It has been expanded with the usability of various social media application using internet networks that can be accessed everywhere, give personal computing power in the pockets of users and at the same time, given them ubiquitous access to rich online social network information (Aaron Beach, 2009).

Large growth in the use of mobile phones especially among the userth were being a trend but unfortunately extensive use of technology can lead to addiction since most of the major social network companies, as well as social content creators, were working hard every day to make their networks so addictive that user can't resist them (Elgan, 2015).

Salehan & Negahban (2013) suggest that the people with larger number of social network friends and higher levels of SNS intensity are more likely to install and use mobile social networking applications on their mobile phones and conclude mobile social networking applications are significant predictor of mobile addiction.

According to the poll conducted by Common Sense Media, (2016), 50% of the teenagers opinion they had an addiction to the mobile device when they spent too much time scrolling on their smartphones from the morning until midnight. While 72% respondent from the poll said they felt the need to immediately respond to texts and social networking messages.

The situation is getting worse when they are in the glue with a smartphone when they holds it at all times while walking, driving, dining, or in the toilet.

## **2.8 Summary**

In this chapter, we have gone through a definition of main term in this topic and brief about component in Facebook such as usage frequency, network size, concern for internet privacy and unwanted audience, also profile visibility. Literature review regarding privacy risk in online social network, awareness of internet privacy, and addiction to mobile social network had been discuss based on previous study and statistic as a wrap for this chapter before continue to research method on the next chapter.



## **CHAPTER 3**

### **RESEARCH METHOD**

#### **3.1 Introduction**

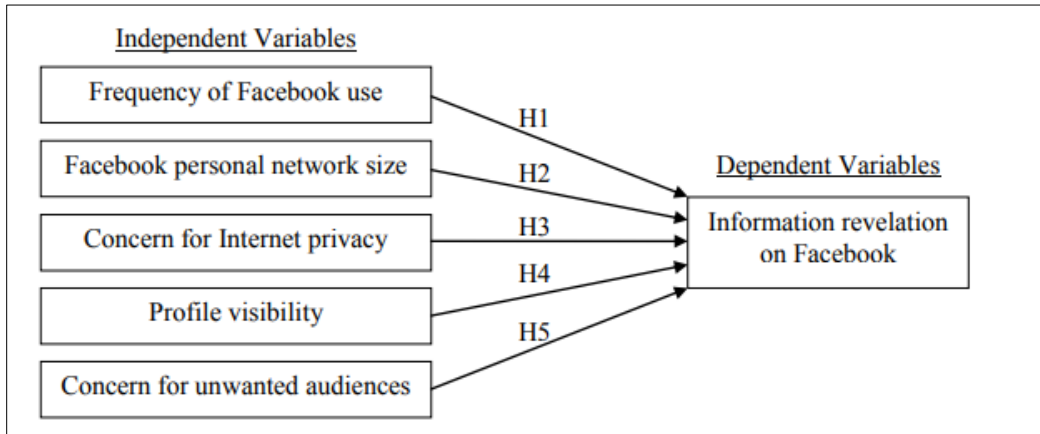
This chapter will explain about independent and dependent variable involves in this research and also research design and procedures counting in. Research framework and variable selection were explained before doing the hypothesis for every profile elements asked in the questionnaire, and each profile elements was estimating having (or not) a relationship with all independent variable (element of profile revelation) .

#### **3.2 Research Framework and Variables Selection**

The theoretical framework was developing to test the phenomena of interest in this study (Ishak, 2012). Theories are formulated to explain, predict, and understand phenomena and, in many cases, to challenge and extend existing knowledge within the limits of critical bounding assumptions and stand as structure to support a theory of this research study (Abend, 2017).

Below are the dependent and independent variables involved in this research. Independent variables taken from the elements of Facebook profile that they reveal in their Facebook account consist of frequency of Facebook log on activity, Facebook personal network size, concern for internet privacy, profile visibility and concern for unwanted audiences while dependent variable was information revelation on Facebook.

Figure 2  
*Theoretical Framework*



Source: Gross & Acquisti,(2005)

### 3.3 Hypothesis Setting

H1: There is a relationship between Facebook log on activity and information revelation on Facebook.

H2: There is a relationship between Facebook personal network size and information revelation on Facebook.

H3: There is a relationship between concern for Internet privacy and information revelation on Facebook.

H4: There is a relationship between profile visibility and information revelation on Facebook.

H5: There is a relationship between concern for unwanted audiences and information revelation on Facebook.

### **3.4 Research design**

Research design was interpreting as a strategy chosen to integrate different components of the study in a coherent and logical way (Abend, 2017) to effectively address the research problem; it constitutes the blueprint for the collection, measurement, and analysis of data. Survey and correlational design was use to investigate how each design can be used to test the same hypothesis (UPM, 2017). Survey interpreted as a series of questions or statements to which participants indicate responses.

In this research, printed forms were used to make it easy to facilitate the distribution of forms and retrieval with the maximum percentage of questionnaire returns within the large group of respondents.

#### **3.4.1 Questionnaire development**

This cross sectional study using survey research and responses are gathered in a standardized way so questionnaires are more objective. Generally it is relatively quick to collect information using a questionnaire (Milne) and suitable to use for a large portion of group of sample or population. Potentially information can be collected from a large portion of a group. Questionnaire is delivered and responded right after they finish filling the data. Using a questionnaire adopted from Govani & Pashley, (2005) for the similar research, data have been collected.

### **3.4.2 Population and sample**

Random sample from 512 students from School of Business Management, Universiti Utara Malaysia was selected to perform this study. About 150 students who are having Facebook account were asked to complete all questions from the questionnaire which are more than 10% from the population by using convenience sampling method.

### **3.5 Instrumentation**

In concern of producing a good questionnaire, this survey written to be as short and concise as possible, yet still able to convey or measure (UPM, 2017) what it is intended to measure. In this study, three parts of questionnaire were count in to produce a raw data which was demographic information such as mobile Facebook log on activity (or not), gender, and age. While part B asking five selected elements that they reveal on their personal account of Facebook including relationship status, birthday, education, photo, and real name which to be used to measure information they reveal to others on Facebook. Part C consists of four question about internet privacy topic to measure concerns of internet privacy in Facebook. Last but not least, part D asking respondent regarding unwanted audiences that might be access their profile without any invitation.

### **3.5.1 Information revelation**

The scale adopted from Govani and Pashley (2005) has supporting these elements to be valid for testing. Respondent were requested to report which element (relationship status, birthday, education, photo, and real name) from their profile they reveal in the Facebook wall so people who connected to them (friend list in Facebook) or public (can be anyone who were having Facebook account – real or fake). Two point scales (“yes” or “no”) were given and respondent only allowed ticking either one of these answer for each Facebook profile elements they reveal.

### **3.5.2 Frequency of Facebook use**

This section asked respondent to report how often they log in to their Facebook account either via mobile phone or website. Two options for the answer were given – log in on daily basis or weekly basis. This question’s was on purpose to investigate frequency of Facebook log on activity by the respondent. This part will be test with the element of information revelation above to investigate relationship between these variables.

### **3.5.3 Personal network size**

This section asked respondent regarding the amount of their friend list in Facebook. Options given were on scaling from 0 to 499 (first option) or 500 and above (second option). Question asked in purpose to know their network size (friend list) in Facebook. This part will be test with the element of information revelation above to investigate relationship between these variables.



#### **3.5.4 Concern for internet privacy**

Questionnaire asked “Do user concern about internet privacy?” and respondent need to answer either “Yes, I am concern about it” or “No, I do not concern about it. This question involved to test relationship of concern level to the element of Facebook profile they reveal; adapted from (Tufekci, 2008) and considered valid and reliable.

#### **3.5.5 Profile visibility**

From a scale adopted from Ellison, (2011), respondent were asked to whom they reveal their profile; 1 = visible for friend only and 2 = visible to public (anyone can access their information including anonymous). This question was on purpose to measure profile revelation by the respondent in their Facebook account profile.

#### **3.5.6 Concern for unwanted audience**

Borrowed from Tufekci,( 2008) research regarding future audiences, seven questions have been asked to the respondent about unwanted audiences they probably face out reviewing their profile such as employers, police, university management, and political parties. Two option of answer were given whether they 1 = agree or 2 = disagree with the situation given to measure level of trust their profile might be access by the parties as above.

### **3.6 Procedures of data collection**

By applying self-administered questionnaire, the data collected using traditional paper and pencil techniques. Everyone was in the same place hearing the same verbal instruction. Each respondent will be given a printed questionnaire that can be filled using a pencil or pen conducted in group setting. Before questionnaire distributed, permission from the lecturer were asked and once granted, a basic briefing about the researcher background, purposes of the data collection and explanation about the question was done. Each person was expected to complete the questionnaire without being consult by others except basic instruction from the researcher. Any question and comments were handled in similar way.

### **3.7 Summary**

Along this chapter, we have investigated research framework – and variable selection which were information revelation on Facebook as dependent variable and five independent variables which are:

- a) Frequency of Facebook log on activity
- b) Facebook personal network size
- c) Concern for internet privacy
- d) Profile visibility
- e) Concern for unwanted audience

From the variables above, we have tested each independent variable with detail that they reveal on their Facebook profile to made hypotheses. The data collected using a set of questionnaire to test the hypotheses as above. Pilot test result are accepted when the

Cronbach Alpha is greater than 0.05 (0.79); data collected from the questionnaire were valid to test.



## CHAPTER 4

### RESULTS

#### 4.1 Introduction

This chapter will discuss about results and analyses from the raw data that have been taken from the respondent as findings of the study. Relevant statistical tests were employed with the main objective to test whether the result of analysis will support the proposed hypothesis. Frequency analysis was run to get the number of occurrences in every variable. This is followed by Chi-square tests to identify the relationship among variables.

#### 4.2 Demography

##### 4.2.1 Respondent status

Table 1  
*Respondent account in Facebook*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	150	100.0	100.0	100.0

First question in the questionnaire was asking about whether the respondent having an account in Facebook website or not. Only Facebook user are allowed to continuing answering the following questions since it's related to the Facebook profile of the respondent. According to the data, 100% of the respondent was Facebook user which was 150 respondents.

#### 4.2.2 Gender

Table 2  
*Frequency of gender*

		gender			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	33	22.0	22.0	22.0
	female	117	78.0	78.0	100.0
	Total	150	100.0	100.0	

Based on the survey, table above reports the frequency of gender among the respondent within undergraduate students in Universiti Utara Malaysia. Male students recorded a total of 33 people with a percentage of 22% from the total 150 respondents while 78% of the respondents were female with the total of 117 people.

#### 4.2.3 Age

Table 3  
*Frequency of age*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	21-25	147	98.0	98.0	98.0
	26-30	2	1.3	1.3	99.3
	36-40	1	.7	.7	100.0
	Total	150	100.0	100.0	

As shown above, most of the respondent (undergraduate students in Universiti Utara Malaysia) were within the range of 21 to 25 years old which was 98% from the total. While the other 1.3% were on the range of 26 to 30 years old and the remaining was in the range of 36 to 40 years old.

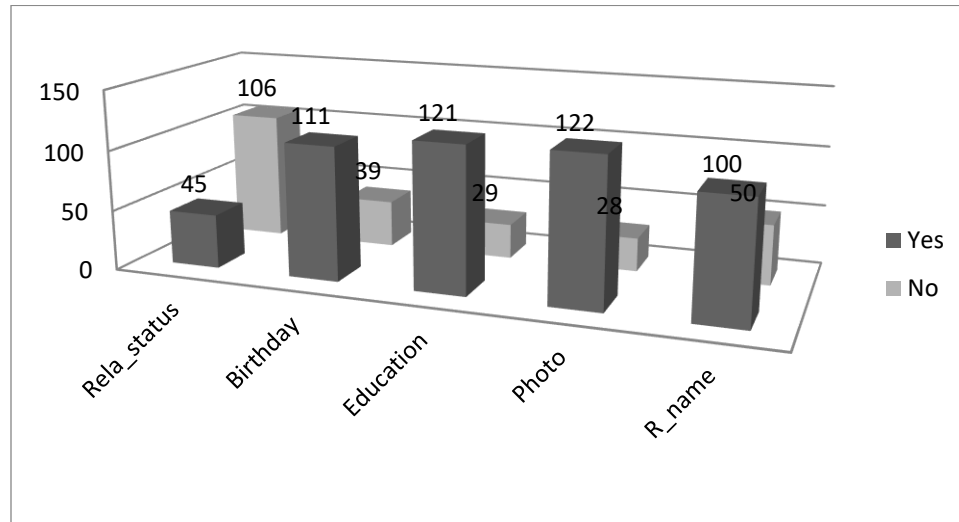
#### **4.3 Information revelation on Facebook**

This part asking respondents regarding the element of profile they reveal on their profile in Facebook. In Facebook profile setting, they can choose whether want to share the information with their friend list only or let everyone can see their personal information online. According to Facebook, (2017), they make some of the information in user's profile to public in purpose to help connect users with friends and family (such as profile photo, age, and current hometown location).

In the other hand, Facebook gives an option to make the profile private or public as a respect to user's privacy. Users can control the audience who can access their relationship status, birthday (user can edit to reveal only date without year or hide it overall), education level (user can choose to hide it at all or only reveal one education centre that they want to), photo ( audience can be set by photo or album), and real names (Facebook encouraging user to use their real name or the name that people know them instead of fake name).

Bar Chart 1

*Information revelation based on Facebook profile elements*



Based on the bar chart, 70% of the respondents were not so comfortable to sharing their relationship status and are more comfortable to make them as private while the remaining 45 respondent was open to use their real name and reveal it to the public. 111 respondents that cover 74% of the overall respondent have no issue to reveal their birthday to the public while 26% more not agree to reveal this sensitive information. Almost 81% was proud to tell public their educational level while the other 29 respondent not interested to share with others. On personal photo, 18.7% of the respondent say no to share their picture while the remaining 122 respondent (81.3%) interested to share their photo to others in Facebook. When it comes to real name, only 66.7% of the respondent were willing to reveal their real name while 50% more comfortable to keep it as a secret.

## 4.4 Usage

### 4.4.1 Log on activity

Bar chart 2

*Log on activity*

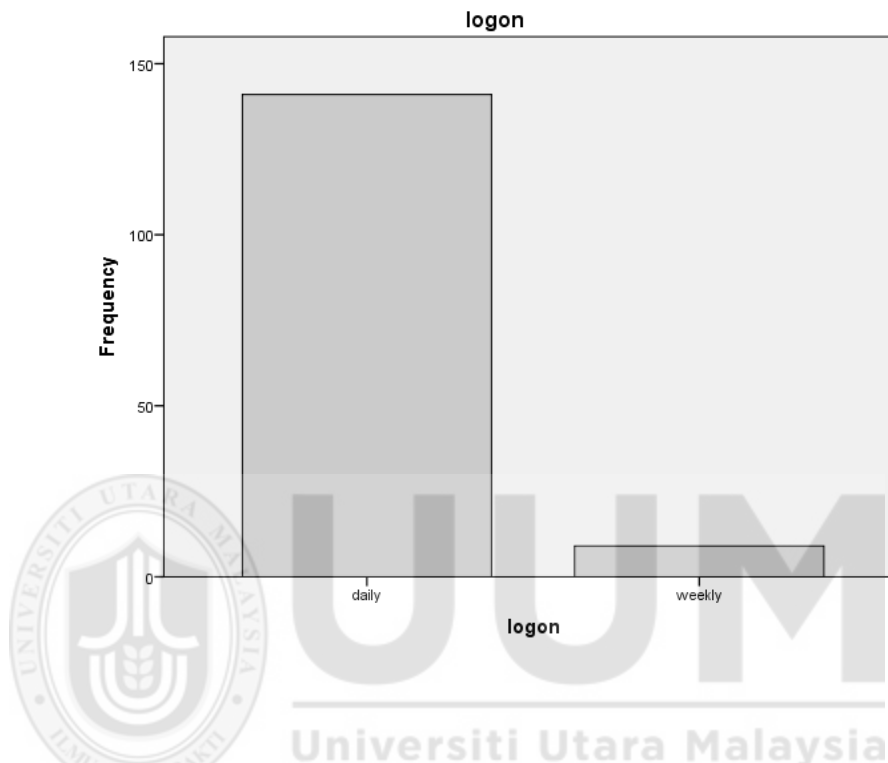


Table 4

*Statistic of Facebook log on activity*

		logon			Cumulative
		Frequency	Percent	Valid Percent	Percent
Valid	daily	141	94.0	94.0	94.0
	weekly	9	6.0	6.0	100.0
	Total	150	100.0	100.0	

According to the data above, most of the respondents were loyal visitor of the Facebook site daily which records the number of 141% that covered 94% of the total respondent. While the rest of 9 respondents were only access Facebook weekly.



#### 4.4.2 Facebook friends and connections

Bar chart 3

*Personal network size*

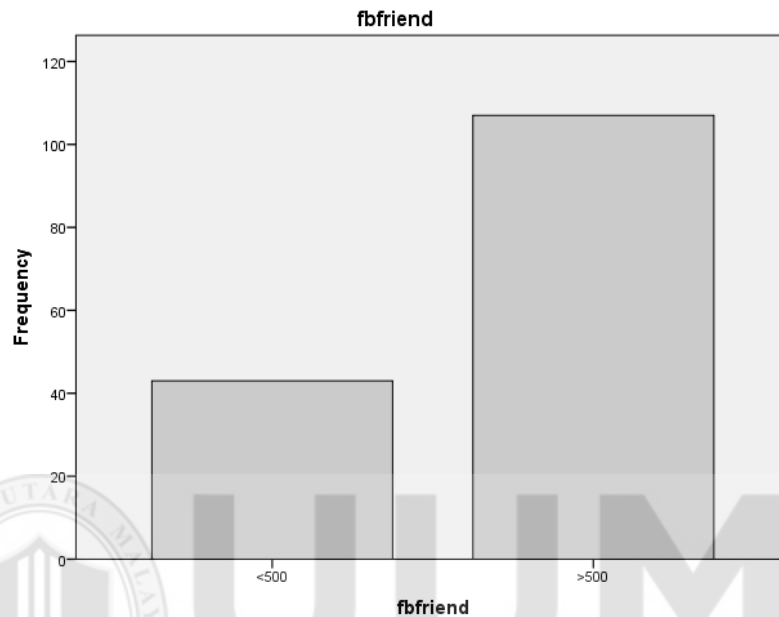


Table 5

*Personal Facebook network size*

		fbfriend			Cumulative Percent
		Frequency	Percent	Valid Percent	
Valid	<500	43	28.7	28.7	28.7
	>500	107	71.3	71.3	100.0
Total		150	100.0	100.0	

Table 5 above shows that only 28.7% of the respondent having less than 500 friends while the other 107 respondents that cover 71.3% having a large network size when their friend list were more than 500 people.

#### 4.4.3 Internet privacy concern

Bar chart 4

*User internet privacy concern*

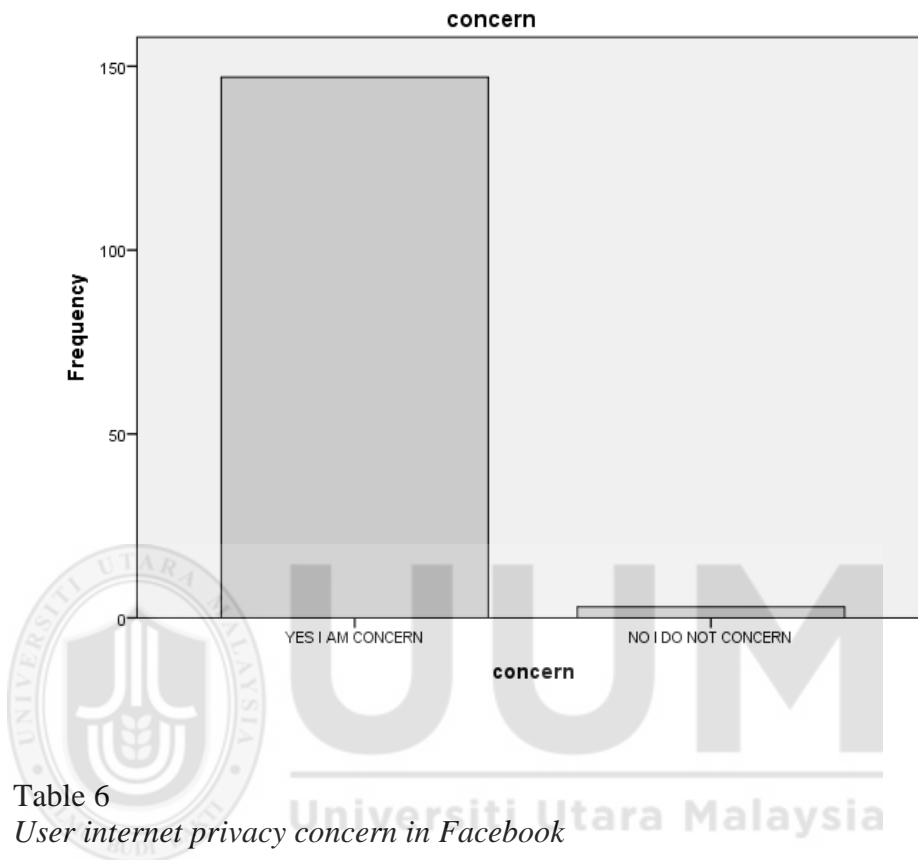


Table 6

*User internet privacy concern in Facebook*

		concern			Cumulative Percent
		Frequency	Percent	Valid Percent	
Valid	yes	147	98.0	98.0	98.0
	no	3	2.0	2.0	100.0
	Total	150	100.0	100.0	

Histogram and table above reports internet privacy concern among respondents that records 98% of respondents (147 person) concern about internet privacy while the other 2% (3 person) don't mind about this matter.

#### 4.4.4 Profile visibility

Bar chart 5

*Frequency of Facebook profile visibility*

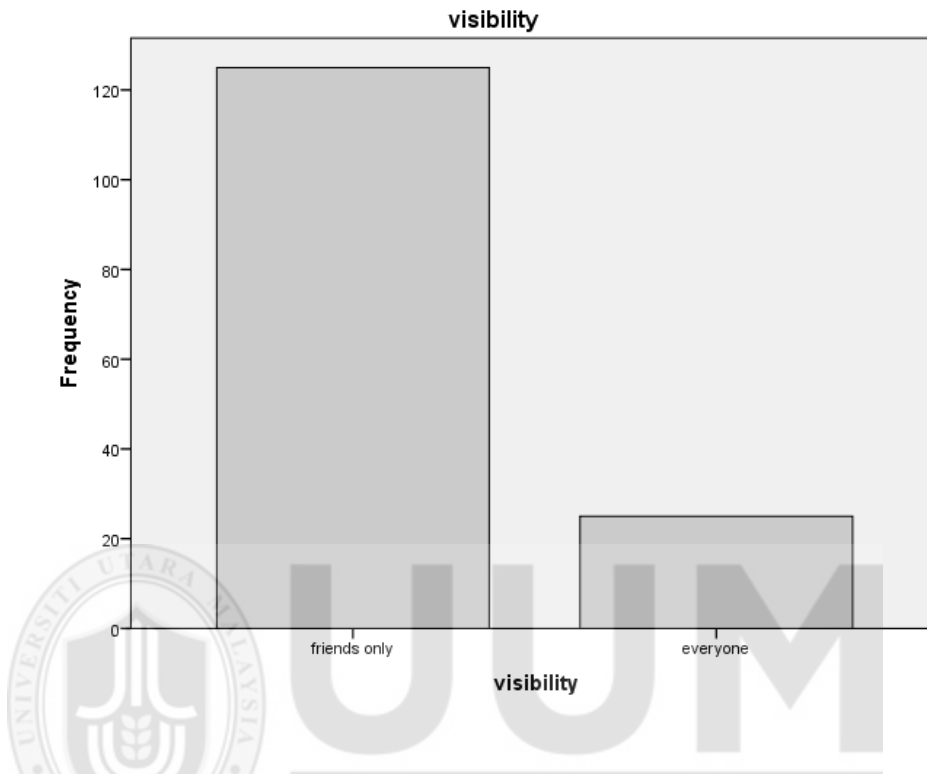


Table 7  
*User's profile visibility*

		visibility			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	friends only	125	83.3	83.3	83.3
	everyone	25	16.7	16.7	100.0
	Total	150	100.0	100.0	

Table 7 shows that majority of the respondent (83.3%) setting their profile only visible to the specific trusted friend list while the other 25 respondent which is cover 16.7% of the total respondent feel open to reveal their profile information to anyone who browsing and accessing Facebook.

## 4.5 Result analysis

In this topic, chi square test were perform to investigate the relationship among variables in order to test the hypothesis made in chapter 3 previously. The Chi-Square test of independence is used to determine if there is a significant relationship between two nominal (categorical) variables where the frequency of each category for one nominal variable is compared across the categories of the second nominal variable (Lani, 2017).

### 4.5.1 Facebook log on activity and information revelation

Analysis result of chi square test below explains whether they are relationship between Facebook login frequencies with Facebook information revelation that have been asked in the questionnaire.

Table 8  
*Facebook log on activity and information revelation*

Chi-Square Tests					
	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	8.055 <sup>a</sup>	1	.005		
Continuity Correction <sup>b</sup>	5.774	1	.016		
Likelihood Ratio	6.286	1	.012		
Fisher's Exact Test				.014	.014
Linear-by-Linear Association	8.001	1	.005		
N of Valid Cases	150				

a. 1 cells (25.0%) have expected count less than 5. The minimum expected count is 1.74.

b. Computed only for a 2x2 table

H1c: There is a relationship between frequency of Facebook log on activity and information revelation

From the analysis above, hypothesis 1 was **accepted** since  $\chi^2 (1, N = 150) = 8.06$ ,  $p < 0.05$

#### 4.5.2 Personal network size and information revelation

Analysis result of chi square test below explains whether there are relationships between personal network sizes (in Facebook) with Facebook information revelation that have been asked in the questionnaire.

Table 9  
*Personal network size and information revelation*

Chi-Square Tests					
	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	5.902 <sup>a</sup>	1	.015		
Continuity Correction <sup>b</sup>	4.843	1	.028		
Likelihood Ratio	6.881	1	.009		
Fisher's Exact Test				.021	.010
Linear-by-Linear Association	5.862	1	.015		
N of Valid Cases	150				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 8.31.

b. Computed only for a 2x2 table

H2: There is a relationship between Facebook personal network size and information revelation

From the analysis above, hypothesis H2 was **accepted** since  $\chi^2 (1, N = 150) = 5.90$ ,  $p < 0.05$ .

#### 4.5.3 Concern for internet privacy and information revelation

Analysis result of chi square test below explains whether there is a relationship between concerns for internet privacy (in Facebook) with Facebook information revelation that have been asked in the questionnaire.

Table 10  
*Internet privacy concern and education level revelation*

Chi-Square Tests					
	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	.734 <sup>a</sup>	1	.392		
Continuity Correction <sup>b</sup>	.014	1	.906		
Likelihood Ratio	1.304	1	.254		
Fisher's Exact Test				1.000	.522
Linear-by-Linear Association	.729	1	.393		
N of Valid Cases	150				

a. 2 cells (50.0%) have expected count less than 5. The minimum expected count is .58.

b. Computed only for a 2x2 table

H3: There is a relationship between concern for Internet privacy and revelation of education information on Facebook.

From the analysis above, hypothesis H3 was **rejected** since  $\chi^2 (1, N = 150) = 0.73$ ,  $p > 0.05$ .

#### 4.5.4 Profile visibility and information revelation

Analysis result of chi square test below explains whether they are relationship between profile visibilities with Facebook information revelation that have been asked in the questionnaire.

Table 11  
*Profile visibility and information revelation*

Chi-Square Tests					
	Value	df	Asymptotic Significance (2- sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)
Pearson Chi-Square	1.034 <sup>a</sup>	1	.309		
Continuity Correction <sup>b</sup>	.547	1	.459		
Likelihood Ratio	1.136	1	.286		
Fisher's Exact Test				.412	.236
Linear-by-Linear Association	1.028	1	.311		
N of Valid Cases	150				

a. 1 cells (25.0%) have expected count less than 5. The minimum expected count is 4.83.

b. Computed only for a 2x2 table

H4: There is a relationship between profile visibility and information revelation

From the analysis above, hypothesis H4 was **rejected** since  $\chi^2 (1, N = 150) = 1.03$ ,  
 $p > 0.05$

#### 4.5.5 Concern for unwanted audiences and information revelation

Analysis result of chi square test below explain whether they are relationship between concern for unwanted audiences in Facebook that may access their profile uninvited such as employers, university, police, sexual predators, and political parties with five elements of Facebook information revelation that have been asked in the questionnaire

Table 12  
*Unwanted audiences and information revelation*

Chi-Square Tests					
	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.069 <sup>a</sup>	1	.793	.836	.476
Continuity Correction <sup>b</sup>	.003	1	.958		
Likelihood Ratio	.068	1	.794		
Fisher's Exact Test					
Linear-by-Linear Association	.068	1	.794		
N of Valid Cases	150				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 12.37.

b. Computed only for a 2x2 table

H5: There is a relationship between concern for unwanted audiences and birth date sharing

From the analysis above, hypothesis H5 was **rejected** since  $\chi^2 (1, N = 150) = 0.069, p > 0.05$



#### 4.6 Correlation Test

This test was done in purpose to investigate about the strength of the linear relationship between two variables for the population of undergraduate students in Universiti Utara Malaysia. Pearson Correlation produces a sample correlation coefficient,  $r$ , which measures the strength and direction of linear relationships between pairs of continuous variables (Kent State University, 2017).

By extension, the Pearson Correlation evaluates whether there is statistical evidence for a linear relationship among the same pairs of variables in the population, represented by a population correlation coefficient,  $\rho$  (“rho”). Correlation matrix done was as an appendix A and selected variable that having high correlation were explained as below:

##### 4.6.1 Gender and information revelation

Table 13  
*Correlation for gender and status*

Correlations			
		gender	status
gender	Pearson Correlation	1	.039
	Sig. (2-tailed)		.639
	N	150	150
status	Pearson Correlation	.039	1
	Sig. (2-tailed)	.639	
	N	150	150

Table 14  
*Frequency of status and gender*

			gender		Total
			male	female	
status	yes	Count	11	34	45
		Expected Count	9.9	35.1	45.0
		% within status	24.4%	75.6%	100.0%
	no	Count	22	83	105
		Expected Count	23.1	81.9	105.0
		% within status	21.0%	79.0%	100.0%
Total	Count	33	117	150	
	Expected Count	33.0	117.0	150.0	
	% within status	22.0%	78.0%	100.0%	

Data above was a result of correlation test between gender and information revelation in Facebook. From the data, the correlation of gender and status was 0.639 which is highly correlated. From the frequency table, we can conclude female respondent were more openness to share their relationship status rather than male respondent.

#### 4.6.2 Log on activity and information revelation

Table 15

*Log on activity and information revelation*

Correlations		logon	fbfriend
logon	Pearson Correlation	1	.036
	Sig. (2-tailed)		.662
	N	150	150
fbfriend	Pearson Correlation	.036	1
	Sig. (2-tailed)	.662	
	N	150	150

Table 16

*Log on activity and information revelation*

			fbfriend		Total
			<500	>500	
logon	daily	Count	41	100	141
		Expected Count	40.4	100.6	141.0
		% within logon	29.1%	70.9%	100.0%
	weekly	Count	2	7	9
		Expected Count	2.6	6.4	9.0
		% within logon	22.2%	77.8%	100.0%
Total		Count	43	107	150
		Expected Count	43.0	107.0	150.0
		% within logon	28.7%	71.3%	100.0%

From the data above, we can conclude that log on activity was highly correlated to network size in scale of 0.662 via correlation test. Taken from the frequency table, 70.9% of Facebook log on activity that having friend list more than 500 people were log on into their Facebook account daily from the total of 141 people who access their Facebook daily.

#### **4.7 Conclusion**

In conclusion, we can summarize that only Facebook log on activity and personal network size having a positive result on chi square test ran as above. The rest were rejected (concern for internet privacy, profile visibility, and concern for unwanted audience). Correlation test were done to the gender and log on activity to information revelation and both are highly correlated where female respondent were reveal more information in Facebook and person who were having big network size (500 and above) were reveal more information about themselves.



## **CHAPTER 5**

### **DISCUSSION AND CONCLUSION**

#### **5.1 Introduction**

This chapter will answer the objective of the study from chapter 1 regarding the relationship between internet privacy concern and Facebook information revelation. Result (from the test) for all the elements asked in the questionnaire was discussed below and the research findings were summarizing in one paragraph solidly. Future research recommendations were included and limitation of the study was explained as below.

#### **5.2 Discussion of findings**

Taken the result of the research in previous chapter, below is the discussion by each variable regarding relationship between each other that have been test in chapter 4 according to the hypothesis build in chapter 3.

##### **5.2.1 Facebook log on activity and information revelation**

One of the questions in the questionnaire has asked the respondent “How often user log on to mobile Facebook?” This question was asked in purpose to know the relationship between frequency of Facebook log on activity and the information revelation that respondent reveal in their profile. From the test had been done in chapter 4, it was found that there is a relationship between frequency of Facebook log on activity and profile revelation elements.

This result were fully support by Tufekci, (2008) that conclude his research; the more often Facebook log on activity log on to their personal account, more information they would like to reveal. Gross & Acquisti, (2005) also in the same ship with Tufekci and support when they found an association between frequency of Facebook log in activity and information revelation in their research (previously before Tufekci) where 82% of Facebook log on activities that actively log on to their account doesn't mind to share their personal information to the public.

### **5.2.2 Facebook personal network size and information revelation**

From the data collected and tested in this research, there is a significant relationship occurs between Facebook personal network size and profile information revelation of the respondent.

This result were support with a study by Jones & Soltren, (2005) that stated the more online friends user had (300 friends and above), more information reveal regarding their interest compared to the person who were having small network size. Userng & Quan-Haase, (2009) also agree with a study by Jones & soltren when their research found similar result mentioned that personal network size was positively associated with Facebook information revelation.

### **5.2.3 Concern for internet privacy and information revelation**

Result shows that there is no relationship between concern for internet privacy and information revelation on Facebook. The finding was parallel to the past research by Userng and Quan-Haase (2009). Userng and Quan-Haase's study showed that general concern for Internet privacy was negatively associated with information revelation on Facebook.

Contrary to Pew (2006) and Viseu et al. (2004) researches, these studies have found that general concern for Internet privacy has an effect on the information revelation behaviors of Internet users. Research by Viseu et al. (2004) has also suggested that individuals with a comparably low level of concern for Internet privacy tend to be much more exposed and open with the disclosure of their personal information online.

As a result of the data analysis in this study, it can be concluded that concern for Internet privacy and information revelation on Facebook has no significant relationship.

#### **5.2.4 Profile visibility and information revelation**

The result of the study showed that there was no relationship between profile visibility and information revelation on Facebook. Contrary to previous research that has been done by Userng and Quan-Haase (2009), they found that profile visibility was positively associated with information revelation. Joinson et al. (2010) also found that trust and perceived privacy had a strong effect on individuals' willingness to disclose personal information to a website.

As a result of the data analysis in this study, it can be concluded that profile visibility and information revelation on Facebook has no significant relationship.

#### **5.2.5 Concern for unwanted audiences and information revelation**

The chi square test showed that there is no relationship between concern for unwanted audiences and information revelation on Facebook and fortunately supported by Userng and Quan-Haase (2009) in his study from a conclusion: concern for unwanted audiences showed no association with information revelation. In the other hand, Acquisti and Gross (2006) found parallel results that students expressed high levels of concern for general privacy issues on Facebook. However, despite these concerns, Acquisti and Gross (2006) has also shown that users continue to disclose personal information and often disclose accurate personal information online (Govani & Pashley, 2005; Gross & Acquisti, 2005; Pew, 2000; Tufekci, 2008).



As a result of the data analysis in this study, it can be concluded that concern for unwanted audience and information revelation on Facebook has no significant relationship.

### **5.3 Suggestion related to mobile Facebook privacy**

Learn about the privacy controls on user's favorite websites and use them (Media Literacy Council, 2018). Connect only with people user know offline - When people try to add user as a connection, if user don't really know them, block them so they can't contact user again. Be mindful about posting personal information - Posting personal information such as user's full name, address, phone number, school, email address, or photos on portals and forums can identify user to strangers and put user's safety at risk. Avoid listing user's name and address on internet directories or job posting sites. Especially important, keep user's account numbers, user names and passwords secret. Think before user post - Once user put something online, it's impossible to take it back. Images, text and videos can be copied and reposted over and over without user knowing. So even if just user's friends can see what user post, that content could end up anywhere on the Web (if they become user's ex-friends or if their profiles are public). User will have a hard time trying to remove it.

Ask friends not to post photos of user or user's family without user's permission. At the same time, refrain from tagging friends in photos or videos online.

Keep an eye on user's digital reputation - Regularly search for user's name to see what comes up. If user find information that isn't true or that shouldn't be public, work with the person who posted it or the hosting website to take it down.

Read the privacy policy of websites that user visit, especially for transactions. Find out what data the website gathers about user, how it is used, shared and secured. If there is no privacy policy, take user's business elsewhere!

Facebook has set various options to protect user data from being used by unscrupulous individuals. Security is built into every Facebook product by offering several security features, such as login alerts and two-factor authentication, to help user add an extra layer of protection to their account. User also can review and update security settings at any time via website or mobile application. For safety, user can make sure they log out from their account and clear cache after using Facebook so other people cannot access to their account.

Facebook suggest user to limit person who can access their profile. Regular checkup were advice to do to make sure no unwanted parties stalking Facebook account. For mobile Facebook, user didn't advised to let their account in log in every time mode since anyone can access the phone; or else, user can set a password to the apps or to the phone itself. User can block or unfriend other account that may harm them. Else, they can report to the Facebook administrator so the Facebook team can investigate any suspected breach of security regarding the case. As shown on figure 11, Facebook always care about the safety of their customer's data.

In addition, using internet explorer as a browser was quite risky compare to Chrome and Mozilla Firefox (Pringle, 2014). According to him, by using Chrome and Mozilla Firefox, user can add on some additional function that so helpful in data security such as Ads Block Plus – function for blocking any unwanted ads so user are less likely to see dangerous links; and Noscript that won't allow a web site to run Javascript unless permission given by the user. Normally Firefox will prevent cross-site linking, which is a practice that hackers use to insert dangerous code within regular looking links.

Clicking unknown link may be harm to user's profile since it is a common practice by malware writers to purchase domain names similar to valid sites, especially commonly misspelled names. In order to avoid typo, user are advised to google the website first and never type it directly from the browser. Normally, malware set up a web site that looks the same as the real site so user can reveal their id and password without knowing they are in danger.

#### **5.4 Future research recommendation**

Further research could seek to expand the present study by examining other user groups, such as high school or primary school students, to see if their information revelation on Facebook differs from those of university students. The greater number of participants is also recommended as with most studies, the more sample participate, the more reliable and robust the collusions can be draw.

#### **5.4 Limitation**

This study shows number of limitations. First, the findings are based on a small and non-representative sample. Second, the information revelation scale is based on a limited number of items. Third, the model needs to include further variables, for example control variables, such as age, gender, and area of study. Fourth, the results of the study can only be generalized to university students.

#### **5.5 Conclusion**

User can choose more careful passwords, limiting where, when and with whom they share sensitive data, and using a VPN to encrypt their data every time they go online (Gorodysky, 2017) and being more selective on approving friend request online. Social networking websites should inform potential users that risk taking and privacy concerns are potentially relevant and important concerns before individuals sign-up and create social networking websites.

The objectives of this research have been achieved and all questions raised were answered. As a conclusion, the results of the findings revealed that Internet privacy concerns did not play any role in tendency of information revelation on Facebook.

## REFERENCE

- Aaron Beach, M. G. (2009). Solutions to Security and Privacy Issues in Mobile Social Networking. *International Conference on Computational Science and Engineering*, (pp. 1036-1042).
- Abend, G. (2017). Retrieved 2017, from University of Southern California:  
<http://libguides.usc.edu/writingguide/theoreticalframework>
- Acquisti, A. (2009). Personal Information Revelation in Online Social Networks.
- Ballings, M. (2015). CRM in social media: Predicting increases in Facebook usage frequency. *European Journal of Operational Research*, 248-260.
- Bianchi, A., & Phillips, J. G. (2005). Psychological Predictors of Problem Mobile Phone Use. *CyberPsychology & Behavior*, 39-51.
- Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer Mediated Communication*, 210–230.
- Cecere, G. (2015). Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting*, 277-287.
- Chung, W. (2002). A snoop at privacy issues on the internet in New Zealand. *Business Review*, pp. 2-16.
- Clarke, R. (1999). Internet Privacy Concern confirm the case for intervention. *Communications of the ACM*, 60-67.
- Cohen, S. (2016). *Huffpost*. Retrieved from Huffington Post:  
[https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-\\_b\\_13006700.html](https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html)
- Common Sense Media. (2009). *Is Technology Networking Changing Childhood? A National Poll*. San Francisco: Common Sense Media.
- Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. 341-363.
- Debatin, B., Lovejoy, J. P., M.A., A.-K. H., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Jprunal of Computer Mediated Communication*, 83–108.
- Dong, Z.-B., Song, G.-J., Xie, K.-Q., & Wang, J.-Y. (2009, April 24). An Experimental Study of Large-Scale Mobile Social Network. *Poster Sessions*, pp. 1175-1176.
- Eldon, E. (2010, February). New Facebook Statistics Show Big Increase in Content Sharing.
- Elgan, M. (2015). *Computerworld*. Retrieved 2017, from  
<https://www.computerworld.com/article/3014439/internet/social-media-addiction-is-a-bigger-problem-than-you-think.html>
- Ellison, N. B. (2011). *Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment*.
- e-Marketer. (2016, April 8). Facebook Remains the Largest Social Network in Most Major Markets. Times Square, New York.
- Facebook. (2017). *Facebook*. Retrieved from  
[https://www.facebook.com/help/167941163265974?helpref=uf\\_permalink](https://www.facebook.com/help/167941163265974?helpref=uf_permalink)
- Finucan, R. (2009). Mobile Social Networking. *Canadian Patent Application* .

- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Journal of Computers in Human Behavior*, 153-160.
- Goforth, C. (2015). *Using and Interpreting Cronbach's Alpha*. Retrieved 2017, from University of Virginia Library: <http://data.library.virginia.edu/using-and-interpreting-cronbachs-alpha/>
- Golijan, R. (2012). *Facebook privacy problems are on the rise*. NBC News.
- Gorodyansky, D. (2017). *Wired*. Retrieved from <https://www.wired.com/insights/2013/10/internet-privacy-and-security-a-shared-responsibility/>
- Govani, T., & Pashley, H. (2005). Student Awareness of the Privacy Implications When Using Facebook. *Privacy Poster Fair at Carnegie Mellon University*.
- Graham, A. (2012). Retrieved 2017, from BigSea: <https://bigsea.co/inbound-marketing/social-media-blog/when-facebook-says-you-have-too-many-friends/>
- 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)*.
- Gwenn Schurigin O'Keeffe, K. C.-P. (2011). *The Impact of Social Media on Children, Adolescents, and Families*. America: The American Academy of Pediatrics Clinical Reports.
- Hall Geisler, K. (2018). *HowStuffWorks*. Retrieved from <https://electronics.howstuffworks.com/cell-phone-apps/facebook-mobile-app2.htm>
- Halle, B. (2015). *History Cooperative*. Retrieved from <http://historycooperative.org/the-history-of-social-media/>
- Hampton, K. N., Sessions, L. F., & Her, E. J. (2010). How Internet and mobile phone use is related to network size and diversity. *Information, Communication, & Society*, 130-155.
- Hassan, Z. A., Schattner, P., & Mazza, D. (2006). Doing A Pilot Study: Why Is It Essential? *Malaysian Family Physician*, 70-73.
- Hodge, M. J. (2007). The fourth ammendment and privacy issues on the new internet : Facebook and Myspace. *Law Journal*, 95.
- Horrigan, J. (2009). *Wireless Internet Users*. Washington DC: Pew Research Center's Internet & American Life Project.
- Houghton, D. J. (2017). Privacy concerns on social networking sites: a longitudinal study. *Joornal of Marketing management*, 1465-1489.
- Iachello, G. (2007). *End-User Privacy in Human-Computer Interaction*. Foundations and Trends.
- Ishak, M. (2012). *Study on information revelation and internet privacy concern on social network sites of Facebook : A case study of non-trained substitute teachers of Universiti Utara Malaysia*. SBM, UUM.
- Johnson, B. (2010, January 11). Privacy no longer a social norm, says Facebook founder. *The Guardian*.
- Johnson, S. (2014). *Solo PR Pro*. Retrieved from <http://soloprpro.com/the-pros-and-cons-of-facebook-mobile-vs-desktop/>
- Jones, H., & Soltren, J. H. (2005). *Facebook : Threat to Pivacy*.

- Jung, Y., & Rader, E. (2016). The Imagined Audience and Privacy Concern on Facebook: Differences Between Producers and Consumers. *Social Media & Society*, 1-15.
- Kane, G. C., Alavi, M., Labianca, G. (., & Borgatti, S. (2012). What's Different About Social Media Networks? A Framework and Research Agenda. *3rd Boston College Social Media Workshop*.
- Kent State University. (2017). *Kent State University*. Retrieved 2017, from SPSS Tutorials: Pearson Correlation: <https://libguides.library.kent.edu/SPSS/PearsonCorr>
- Kerlinger, F. N. (2000). *Foundations of behavioral research (4th edition)*. Harcourt College Publishers.
- Kietzmann, J. H., McCarthy, I. P., Hermkens, K., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 241-251.
- Kowalski, K. (2015). Too many Facebook friends?
- Krishnamurthy, B., & Wills, C. E. (2008). Characterizing Privacy in Online Social Networks. *WOSN'18*. Seattle, Washington, USA.
- Lani, J. (2017). *Non para chi square*. Retrieved 2017, from Chi-Square Test of Independence: <http://www.statisticssolutions.com/non-parametric-analysis-chi-square/>
- Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). *Social Media & Mobile Internet Use Among Teens and Young Adult*. Washington DC: Pew Internet & American Life Project.
- Leonard, H. (2013, Mac 6). *This Is What An Average User Does On Facebook*. Retrieved from Business Insider: <http://www.businessinsider.com/what-does-an-average-facebook-user-do-2013-3/?IR=T>
- Li, M., Cao, N., & Yu, S. (2011). Privacy-preserving personal profile matching in mobile social networks. *INFOCOM, 2011 Proceedings*. China.
- Lim, E. (2000). Electronic Commerce and the Law.
- Lin, h., & Qiu, L. (2012). Sharing Emotion on Facebook: Network Size, Density, and Individual Motivation. *ACM*, 1-6.
- Lund, A. (2013). *Laerd*. Retrieved 2017, from <https://statistics.laerd.com/spss-tutorials/linear-regression-using-spss-statistics.php>
- Madden, M. (2013). *Teens, Social Media, and Privacy*. Pew Research Centre.
- McCandlish, S. (2001). *EFF's Top 12 Ways to Protect Your Online Privacy*. Retrieved from <[http://www.eff.org/Privacy/eff\\_privacy\\_top\\_12.html](http://www.eff.org/Privacy/eff_privacy_top_12.html)>
- MCMC. (2016). *Internet user survey 2016*. Malaysia: MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION.
- Media Literacy Council. (2018). *Online Safety - Sharing Personal Information Online*. Retrieved from Media Literacy Council, Singapore: <https://www.medialiteracycouncil.sg/Online-Safety/Sharing-Personal-Information-Online>
- Mei-Pochtler, D. A. (2017, July). *The Statistic Portal*. Retrieved 2017, from Statista: <https://www.statista.com/statistics/558698/number-of-mobile-internet-user-in-malaysia/>

- Mekovec, R., & Vrcek, N. (2011). Factors that influence Internet users' privacy perception. *33rd International Conference on Information Technology Interfaces*, (pp. 227-232).
- Miller, S. (1997). Privacy and the internet. *Journal of Research and Practice in Information Technology*, 12-15.
- Milne, J. (n.d.). Questionnaires : Some advantages and disadvantages. In *Evaluation Cookbook* (p. 52). Centre for CBL in Land Use, and Environmental Sciences, Aberdeen University.
- Muffet, T. (2014). *Visually*. Retrieved 2017, from <https://visual.ly/community/infographic/social-media/social-media-intensity-mobile-phones>
- Mushtaq, A. (2008). Privacy in Online Social Networks. *Seminar on Internetworking*.
- Negahban, M. S. (2013). Social networking on smartphones: When mobile phones become addictive. *Computers in Human Behavior*, 2632-2639.
- Pringle, B. (2014). *Facebook security issues*. Retrieved from <https://billpringle.com/home/facebook.html>
- Randy Baden, A. B. (2009). Persona: An Online Social Network with User-Defined Privacy. *SIGCOMM'09*. Barcelona, Spain.
- Regan, K. (2003, January 2). Online Privacy Is Dead – What Now? Reputation Defender. (2016, Oct 26). *Privacy*. Retrieved from Reputation Defender: <https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private>
- Rouse, M. (2010, Aug). *TechTarget*. Retrieved from Whatis: <https://whatis.techtarget.com/definition/Facebook-Mobile>
- Ruth N. Bolton, A. P. (2013). Understanding Generation Y and their use of social media: a review and research agenda. *Journal of Service Management*, 245-267.
- Sadeh, N. (2008). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 401-412.
- Saieed, Z. (2017). *Cybercrime surge in Malaysia*. Kuala Lumpur: The Star Newspaper.
- Salehan, M., & Negahban, A. (2013). Social networking on smartphones: When mobile phones become additive. *Computers in Human Behavior*, 2632-2639.
- Smith, I., & Holmes, N. (2005). Social-mobile applications. *Computer*, 84-85.
- Smith, K. (2018, March 5). 47 Incredible Facebook Statistics and Facts. Brighton.
- Smith, M., Szongott, C., & Henne, B. (2012). Big data privacy issues in public social media. *6th IEEE International Conference*. Campione d'Italia, Italy.
- Statista. (2018). *Device usage of Facebook users worldwide as of January 2018*. New York: The Statistic Portal.
- Sterling, G. (2016). *Marketing Land*. Retrieved 2017, from <https://marketingland.com/facebook-usage-accounts-1-5-minutes-spent-mobile-171561>
- Superhighway, P. i. (2005, September). Retrieved from <http://www.privacyrights.org/fs/fs18-cyb.htm>
- Tamara Dinev, P. H. (2004). Internet Privacy, Social Awareness, And Internet Technical Literacy – An Exploratory Investigation . *BLED 2004 Proceeding*, (pp. 1-13).
- Tan, X. (2012). Impact of privacy concern in social networking web sites. *Internet Research*, 211-233.



- Taraszew, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010). Disclosure the personal and contact information by young people in social networking sites: An analysis using Facebook profile as an example. *International Journal of Media and Cultural Politics*, 81-101.
- Taylor, C. (2013, Mar 28). *CNN*. Retrieved from <https://edition.cnn.com/2013/03/28/tech/mobile/survey-phones-facebook/index.html>
- Taylor, D. G., Pentina, I., & Voelker, T. a. (2011). Mobile Application Adoption By Young Adults: a Social Network Perspective. *International Journal of Mobile Marketing*, 60-70.
- Teijlingen, E. R., & Hundley, V. (2001). Social Research Update. *Issue 35*, pp. 1-12.
- Tufekci, Z. (2008, April 22). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, pp. 20-36.
- UPM. (2017). chapter 8: Survey and Correlational Research Designs. In *Binaries* (pp. 225-259). UPM. Retrieved 2017, from [https://www.sagepub.com/sites/default/files/upm-binaries/57732\\_Chapter\\_8.pdf](https://www.sagepub.com/sites/default/files/upm-binaries/57732_Chapter_8.pdf)
- Velven, M. v., & Emam, K. E. (2013). "Not all my friends need to know": a qualitative study of teenage patients, privacy, and social media. *Informatic in Health*, 16-24.
- Wallace, K. (2016). *Half of teens think they are addicted to their smartphones*. US: CNN.
- Walther, Tom, S., Brandon, T., Heide, V. D., Langwell, L., & B., J. (2008). Too Much of a Good Thing? The Relationship Between Number of Friends and Interpersonal Impressions on Facebook. *Journal of Computer Mediated Communication*, 190-211.
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 193.
- Young, A. L., & Quan-Haase, A. (2009). Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook., (pp. 265-273).
- Zimmerman, R. (2001). The way the cookies crumble: internet privacy. *New York University Journal of Legislation and Public Policy*, 2000-2001.
- Ziv, N. D., & Mulloth, B. (2006). An Exploration on Mobile Social Networking: Dodgeball as a Case in Point. *International Conference on Mobile Business*. Computer Society.

### Pilot Test Results

Reliability test was run to measure the internal consistency of the data. Taking the words of Teijlingen & Hundley, (2001), pilot test was a crucial element of a good study design and increase the likelihood by fulfill a range of important functions. In order to obey the rules of research protocols, data collection instruments, sample recruitment strategies, and other research techniques in preparation for a larger study (Hassan, Schattner, & Mazza, 2006), Cronbach Alpha value from SPSS were referred in purpose to measure the strength of consistency. Many methodologists recommend a minimum  $\alpha$  coefficient between 0.65 and 0.8 (or higher in many cases);  $\alpha$  coefficient that are less than 0.5 are usually unacceptable (Goforth, 2015). In this research, pilot test had done to the data collected and below are the result of Cronbach Alpha:

#### *Reliability test (Cronbach Alpha)*

Reliability Statistics	
Cronbach's Alpha	N of Items
.790	25

Hence, from the table above, we can see that the value of alpha is 0.79 which was near to 1. So, the data is reliable and valid to further this research.