THE EFFECTS OF PRIVACY AWARENESS, SECURITY CONCERNS AND TRUST ON INFORMATION SHARING IN SOCIAL MEDIA AMONG PUBLIC UNIVERSITY STUDENTS IN SELANGOR

ARA ANJUMAN

SULTAN IDRIS EDUCATION UNIVERSITY

2023

THE EFFECTS OF PRIVACY AWARENESS, SECURITY CONCERNS AND TRUST ON INFORMATION SHARING IN SOCIAL MEDIA AMONG PUBLIC UNIVERSITY STUDENTS IN SELANGOR

ARA ANJUMAN

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

DISSERTATION PRESENTED TO QUALIFY FOR A MASTERS OF MANAGEMENT
(RESEARCH MODE)

FACULTY OF MANAGEMENT AND ECONOMICS
SULTAN IDRIS EDUCATION UNIVERSITY

2023

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

UPSI/IPS-3/BO 32
Pind : 00 m/s: 1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

Please tick (√)	
Project Paper	
Masters by Research	√
Master by Mixed Mode	
PhD	

INSTITUTE OF GRADUATE STUDIES
DECLARATION OF ORIGINAL WORK

This declaration is made on the 15 August 2022

i. Student's Declaration:

I'm ARA ANJUMAN, MATRIC NO. M20172001589, FACULTY OF MANAGEMENT AND ECONOMICS hereby declare that the work entitled THE EFFECTS OF PRIVACY AWARENESS, SECURITY CONCERNS AND TRUST ON INFORMATION SHARING IN SOCIAL MEDIA AMONG PUBLIC UNIVERSITY STUDENTS IN SELANGOR is my original work. I have not copied from any other students' work or from any other sources except where due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

Anjuman Ara

Signature of the student

ii. Supervisor's Declaration:

I ASSOCIATE PROFESSOR DR ZURAIDAH ZAINOL (SUPERVISOR'S NAME) hereby certifies that the work entitled THE EFFECTS OF PRIVACY AWARENESS, SECURITY CONCERNS AND TRUST ON INFORMATION SHARING IN SOCIAL MEDIA AMONG PUBLIC UNIVERSITY STUDENTS IN SELANGOR(TITLE) was prepared by the above named student, and was submitted to the Institute of Graduate Studies as a * partial/full fulfillment for the confermentof MASTER OF MANAGEMENT (MANAGEMENT INFORMATION SYSTEM)
(PLEASE INDICATE THE DEGREE) and the aforementioned work, to the best of my knowledge, is the said student's work.

29/05/2023
Date

Signature of the Supervisor

UPSI/IPS-3/BO 31
Pind.: 01 m/s:1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

INSTITUT PENGAJIAN SISWAZAH /
INSTITUTE OF GRADUATE STUDIES

BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM

Tajuk / *Title*: **THE EFFECTS OF PRIVACY AWARENESS, SECURITY CONCERNS AND TRUST ON INFORMATION SHARING IN SOCIAL MEDIA AMONG PUBLIC UNIVERSITY STUDENTS IN SELANGOR**

No. Matrik /*Matric's No.*: **M20172001589**

Saya / *I* : **ARA ANJUMAN**

(Nama pelajar / *Student's Name*)

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris
2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of reference and research.
3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.
4. Sila tandakan (√) bagi pilihan kategori di bawah */ Please tick (√) for category below:-*

☐	**SULIT/*CONFIDENTIAL***	Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / *Contains confidential information under the Official Secret Act 1972*
☐	**TERHAD/*RESTRICTED***	Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restircted information as specified by the organization where research was done.*
☑	**TIDAK TERHAD / *OPEN ACCESS***	

Anjuman Ara

(Tandatangan Pelajar/ Signature)

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

ASSOCIATE PROFESSOR DR. ZURAIDAH ZAINOL
Associate Professor of Marketing
Faculty of Management & Economics
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak

Tarikh: **04/05/2023**

Catatan: Jika Tesis/Disertasi ini **SULIT @ TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

ACKNOWLEDGEMENT

In the name of Almighty Allah, the All-Wise, the Merciful

First of all, I thank ALLAH the Almighty from the core of my heart for guiding and inspiring me. All good and nice things that I have had in my life are due to His Help, Love and Mercy. Alhamdulillah, by the grace of Allah, I manage to complete this research. I'm really thankful to my mentor and supervisor Associate Professor Dr Zuraidah Zainol for her endless support and guidance throughout this journey. It wouldn't be possible without her direction & motivation which has encouraged me to get this ability. I would like to also thank all respected faculty members for their countless assistance in every situation during my studies at Sultan Idris Education University, Malaysia. Particularly, I also want to say thanks to the institute of graduate studies (IGS) for being so humble and supportive to me on completion of my studies. Special thanks goes to the respondents who have participated in my research work. Last but not least, I am grateful to family members who believed me and encouraged to complete this work indeed. I am really thankful to my husband Ali Mohammad Haider for being a great support and motivation to me at all time.

ABSTRACT

The purpose of this research was to determine the effect of privacy awareness on security concerns, the effect of privacy awareness and security concerns on trust and the effect of privacy awareness, security concerns and trust on information sharing in the social media platform. This study employed a quantitative method. Data were collected from a sample of 373 public university students, in the age range of 18 to 29 years old in Selangor using an online questionnaire. To analyze the data, descriptive analysis and covariance-based structural equation modeling (CB-SEM) were used. Based on the R^2 value, 17.0 per cent of the total variance in security concerns (SC) is explained by privacy awareness (PA), 6.0 per cent of the variance in the trust is explained by PA and SC, while 27.0 per cent of the variance in information sharing (IS) is explained by PA, SC and trust. The findings showed the significant positive effects of PA on trust ($\beta=0.273$, $p<0.05$), trust on IS ($\beta=0.447$, $p<0.001$), and PA on SC ($\beta=0.464$, $p<0.001$). The findings also indicated the significant negative effect of SC on trust ($\beta=-0.227$, $p<0.05$) and PA on IS ($\beta=-0.400$, $p<0.001$). The effect of SC on IS ($\beta=-0.020$, $p>0.1$) is not significant. In conclusion, to promote IS in social media platforms, trust is the dominant factor that should be enhanced, in which privacy awareness could promote trust, but security concerns weaken the trust. In implication, the findings provide the service providers and sellers with useful information on the elements of privacy, security and trust that need to be emphasized to encourage users to share their information online.

PENGARUH KESEDARAN PRIVASI, KEPRIHATINAN KESELAMATAN DAN KEPERCAYAAN TERHADAP PERKONGSIAN MAKLUMAT DI MEDIA SOSIAL DALAM KALANGAN PELAJAR UNIVERSITI AWAM DI SELANGOR

ABSTRAK

Tujuan penyelidikan ini adalah untuk menentukan pengaruh kesedaran privasi terhadap kebimbangan keselamatan, pengaruh kesedaran privasi dan kebimbangan keselamatan terhadap kepercayaan, serta pengaruh kesedaran privasi, kebimbangan keselamatan dan kepercayaan terhadap perkongsian maklumat dalam platform media sosial. Kajian ini menggunakan kaedah kuantitatif. Data dikumpul daripada sampel yang terdiri daripada 373 orang pelajar universiti awam, dalam julat umur 18 hingga 29 tahun, di Selangor dengan menggunakan soal selidik dalam talian. Bagi menganalisis data, analisis deskriptif dan pemodelan persamaan struktural berasaskan kovarian (CB-SEM) telah digunakan. Berdasarkan nilai R^2, 17.0 peratus daripada jumlah variasi dalam kebimbangan keselamatan (SC) berupaya dijelaskan oleh kesedaran privasi (PA), 6.0 peratus daripada variasi dalam kepercayaan dijelaskan oleh PA dan SC, manakala 27.0 peratus daripada variasi dalam perkongsian maklumat (IS) dijelaskan oleh PA, SC dan kepercayaan. Dapatan menunjukkan pengaruh signifikan dan positif PA terhadap kepercayaan (β=0.273, $p<0.05$), kepercayaan terhadap IS (β=0.447, $p<0.001$), dan PA terhadap SC (β=0.464, $p<0.001$). Dapatan juga menunjukkan bahawa terdapat pengaruh negatif yang signifikan SC terhadap kepercayaan (β=-0.227, $p<0.05$), dan PA terhadap IS (β=-0.400, $p<0.001$). Pengaruh SC ke atas IS (β=-0.020, $p>0.1$) adalah tidak signifikan. Kesimpulannya, untuk mempromosikan IS dalam platform media sosial, kepercayaan ialah faktor dominan yang harus dipertingkatkan, di mana kesedaran privasi boleh mempromosikan kepercayaan, tetapi kebimbangan keselamatan melemahkan kepercayaan. Secara implikasinya, dapatan ini menawarkan pembekal perkhidmatan dan penjual dengan maklumat berguna tentang elemen privasi, keselamatan dan kepercayaan yang perlu dititikberatkan untuk menggalakkan pengguna berkongsi maklumat mereka atas talian.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AMOS	Analysis of Moment Structure
AVE	Average Variance Extracted
CB-SEM	Covariance-based Structural Equation Modeling
CFA	Confirmatory Factor Analysis
CFA	Comparative Fit Index
Covid-19	Coronavirus Disease 2019
CPM	Communication Privacy Management
CR	Construct Reliability
DF	Degree of Freedom
E-commerce	Electronic Commerce
EFA	Exploratory Factor Analysis
GFI	Goodness of Fit Index
GOF	Goodness of Fit
IS	Information System
IS	Information Sharing
KMO	Kaiser-Meyer-Olkin
MCMC	Malaysian Communications and Multimedia Commission
OSN	Online Social Networks
PA	Privacy Awareness
PCA	Principal Components Analysis
PhD	Doctor of Philosophy
PLS-SEM	Partial Least Squares Structural Equation Modeling

RMSEA	Root Mean Square Error of Approximation
SC	Security Concerns
SEM	Structural Equation Modelling
SET	Social Exchange Theory
SNS	Social Networking Sites
SPSS	Statistical Package for Social Sciences
SRMR	Standardized Root Mean Square Residual
T	Trust
TLI	Tucker-Lewis Index
UIAM	Universiti Islam Antarabangsa Malaysia
UiTM	Universiti Technology Mara
UKM	Universiti Kebangsaan Malaysia
UPM	Universiti Putra Malaysia
$\chi 2$	Chi-Square

APPENDIX LIST

CHAPTER 1

INTRODUCTION

1.1 Introduction

Social media is the platform where users share their information, exchange thoughts and engage in online content modification. A number of internet-connected people all over the world are using social media (Aljohani, Nisbet & Blincoe, 2016). This chapter will discuss the introductory part of the research. Basically, it includes the background of the study, research problem and objectives of the study, research questions, hypotheses, operational definitions, research structure and summary.

1.2 Research Background

According to Clement (2020), the social media penetration rate was 49 per cent globally. East Asia was ranked highest for social media penetration with a rate of 71 per cent throughout the world. However, Bernama (2019) has shown in their latest digital report that, Malaysia was ranked top five globally and highest in Southeast Asia for mobile social media penetration. According to Reddy and Reddy (2019), social media is a vital medium of communication which is expanding extremely. Social media users can communicate with each other without meeting (Skeels & Grudin, 2009). People can create their own profiles and share or exchange information about themselves and new ideas with friends on social media platforms. According to Cheung, Lee, and Chan (2015), on social media, users are sharing their personal information, exposing images, updating positions, and exposing particular preferences and involvements. People generally socialize all over the world through social media by sharing their knowledge and experience. In the current era, everyone shares personal information to their own preferences in well-developed social media stages (Benson, Saridakis & Tennakoon, 2015). Dhawan, Singh and Goel (2014) stated that social media are becoming an extreme attraction for users nowadays. Some popular social media platforms like Facebook, Instagram and Twitter are attracting the attention of millions of users nowadays.

Tess (2013) stated that social media platform has become a very effective communication platform which provides us many advantages. According to Mustafa and Hamzah (2011), the usage of social media has increased in the community. As reported by the Malaysian Communications and Multimedia Commission (MCMC) in

Internet User Survey 2018, users in the age group of 20 until 30 years old were recorded as the highest daily users of the Internet. Social networking sites are the top visited websites in Malaysia. They spent about eight hours per day to be online. The study indicates the young generation is the most active among all internet users. The younger generation is using social media for learning, entertainment and social purposes extensively. The aggressive advancement of social media has become an essential field for teens and adolescent communities where they concentrate more and more massive quantity of time (Livingstone, Mascheroni, Ólafsson, & Haddon, 2014). Therefore, social media become an important tool and an easy path for everyone to communicate and exchange information with each other (Dhawan et al., 2014).

Dhawan et al. (2014) stated that social media provides us opportunities for advanced communication. However, in social media, the exchange of information with each other could be misused. Although social networking sites provide us security and privacy to maintain and assure our personal information from unlawful people on sites, still the rules are violated and actual users are unaware of the danger and how to prevent the issues. According to a study by Lenhart et al. (2015) it is found that over 71 per cent of adolescents use numerous social media platforms for self-presentation online. Greenwood et al. (2016) found nearly 90 per cent of adolescents in the age range of 18 to 29 years old hold an active Facebook account and check their accounts numerous times a day and young adults are the most likely to use social media. Many researchers have been concentrating on Internet practices and secure Internet utilization since it is increased massively. In a research done in Turkey and Europe, it is found that the majority of youngsters' internet skills are inadequate and they are disclosed to many online risks, which require families,

schools, policymakers and internet service providers to save their children from the dangers of the internet (Kasikci, Cagiltay, Karakus, Kursun & Ogan, 2014).

According to Reddy et al. (2019), social media are gaining popularity day by day, and a huge amount of data are available to collect from these platforms. It has become a great way for malicious users to collect all genuine users' data. According to the New York Times report, more than five million Facebook users' personal information access were obtained from Cambridge Analytica, which is a political data firm. Another report by D. Ingram says, there was a leak of personal information of Facebook users in 2018.

According to the RiskBasedSecurity (2020) report, a social media marketing company's security incident resulted in the compromise and partial release of over 100,000 social media influencers' personal details. Furthermore, the investigation highlighted that there were an additional 250,000 social media users whose complete personal information was made available on the dark web as a result of this privacy breach. In addition, according to Pew Research Center's 2018 survey, 80% of social media users were concerned that commercial enterprises and internet marketers might access their personal details on these platforms. Furthermore, 74% of individuals think it is crucial for them to have control over who has access to their personal data. However, individuals are still engage in the platform extensilvely, due to increased number of business are connected to social media sites. Social media connections between businesses and shoppers allow for an exchange to take place when consumers provide personal information while making an online exchange. And due

to this circumstance, users share the information without proper understanding of privacy, and this leads them to be vulnerable to security hacks (Fox & Royne, 2018).

Social media users also may obtain privacy violations of users' personal information which they share on social media platforms with others and it also overlays a ground for attack by the malware authors wherever they will unfold malicious code by taking advantage of the users' inherent trust in their social networks (Saleh, Zakaria & Mashour, 2016). Most people click on almost every source they see shared on social media and probably they add anyone to their private network asking for it without realizing who is really behind it (Saleh et al., 2016). Although the users' trust has a significant effect on their decisions about believing or not believing in the information shared by others, the most common threat is the enormous number of users on social media networking sites. World's one of the largest social media platforms MySpace has a poor reputation in terms of the trust. Using of that site was tried to prohibit by many schools and it was also claimed by the law and enforcement officials that, it's being used by sexual predators to target teens (Schrobsdorff, 2006). Boundary instability is assumed to exist because, without the owner's consent, any information should not be shared. This could be prompted by the violation of privacy management and communication trust management (Zlatolas, Welzer, Hölbl & Heriˇ, 2019).

Willoughby and Mark (2018) highlighted that the usage of social media will expose young individuals to a high risk of privacy and security issues. It is important to use social media properly and inform youngsters and families about the risks that can occur in the usage of social media. A study on Internet usage found that most

Malaysian young adults suffer from cyber-bullying online which has an impact on their psychological and clinical health (Yuen Meikeng, Lim May Lee & Clarissa Say, 2018). According to Cybersecurity Malaysia's CEO Datuk Dr Amirudin Abdul Wahab, more than 80 per cent of underage in Malaysia go online from their home. That's the reason cyber parenting is essential to ensure that their kids are gaining good internet courtesy and that helps to get benefits from using the internet while staying safe online (Yuen Meikeng et al., 2018).

According to Nurul Madiha and Mohd Azul (2015), cyber security has become a threat to online platform users because the personal information of users becomes public information and is used for wrong purposes. According to Haris, Sarijan, and Hussin (2017), although people in Malaysia are aware of the dangers of cyberattacks, but they are doing nothing to secure themselves from being assaulted. Cybercriminals search for new Internet technologies and user adaptations to make openings for user attacks, particularly on mobile devices. Malaysians are increasingly using the internet as a form of communication. As a result of this, Malaysia is regarded as the most popular target for cyberattackers (Haris et al., 2017). According to the data below, Malaysia is at number five (5) among the most vulnerable country to cybercrime.

Table 1.1

Malaysia Rank Fifth in Most Vulnerable to Cybercrime

10 Riskiest Countries			
Country	TER	Country	TER
1. Indonesia	23.54%	6. India	15.88%
2. China	21.26%	7. Mexico	15.66%
3. Thailand	20.78%	8. UAE	13.67%
4. Philippines	19.81%	9. Taiwan	12.66%
5. Malaysia	**17.44%**	10. Hong Kong	11.47%

Threat exposure rate (TER): Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over three months.

Source: Haris et al. (2017)

According to the list above, it is clear that Asian nations are more frequently targeted for cyberattacks than western nations. Online bullying, fraud, email scams, ransom, digital piracy, hackers, internet banking, etc. are examples of threat types that are frequently encountered. Cybercrime appears to be most frequently committed through phishing. Due to their inability to recognise phishing emails, most Malaysians suffered negative effects. A cyberattack involving ransomware, known as "WannaCrypt," occurred in 2017. A sort of malicious software called ransomware is intended to prevent use of a computer system until a certain amount of money is paid. According to Cyber Security Malaysia, the attack may result in a temporary or permanent loss of information and the organization's reputation (Haris et al., 2017).

In a report by Yuen Meikeng et al. (2018), it is revealed that in Malaysia social media users are being abused and given rise to scams. According to Reddy et al.

(2019), malicious users produce a large number of spam messages and spread through social media sites which mislead genuine users. These spammers use their own tricks to make traps for original users with misinformation and publicity. This situation exists because social media users are not aware of privacy and do not realize the sharing information risks while using social media (Nurul Madiha & Mohd Azul, 2015). Despite the risk associated with disclosure, users frequently provide their personal information online, since the growing popularity of cyberspace, particularly in a COVID-19 world. It is crucial to understand adequately what causes users' to disclose information. It can be due to the importance of online transactions or any other important online interactions, users have to share their personal information. Thus, it is crucial to understand what affects the result. And it is critical to understand the safeguards underlying these dynamics (Pantano, Pizzi, Scarpi, & Dennis, 2020; Sheth, 2020).

According to Ahmad (2019), the awareness of data privacy is still new yet important to be focused on. The rapid changes in technology and the highest usage of the internet among the young generation are the reasons why awareness is important. They are being exposed to multiple upcoming risks and threats from internet abuses and unauthorized uses of personal information. The lack of understanding on protecting information privacy has opened opportunities for privacy intrusion. Thus to prevent the issue of privacy awareness about information is essential.

Malaysia is ranked 33 globally in terms of social media scams (Symantec, 2016). Identity theft, credit card fraud, unauthorized use of personal data and cybercrimes are among the issues arisen (Barrett-Maitland et al., 2016). The Federal

Trade Commission of the United States has recorded identity theft as the top consumer complaint (Garrison & Ncube, 2011). Individual, government sectors and private industries have lost a vast amount of money as well as reputation damage from these new types of crimes. If such issues are not solved immediately, it will affect the community and communication system. To solve this issue the online platforms should develop users' assurance that the services are providing proper security which is secured to preserve users' personal information (Aldhafferi et al., 2013). At the same time, in order to prevent becoming a victim of personal information breach, online platform users' must be aware of the risks of sharing personal information on the sites and make the wise decision to reveal personal information only when necessary. Thus, these issues led to the conduct of the current study to advance the understanding of young generations' privacy awareness, security concerns and trust in information sharing on social media platforms in Malaysia.

1.3 Problem Statement

Social networking sites continue increasing their popularity (Dhawan et al., 2014). In the digital era, concerns over privacy and security breaches are rampant (Vemprala & Dietrich, 2019). Social media provides us with many advantages but along with that, there are many disadvantages and one of which is the issue of privacy and security (Ali et al., 2018). To maintain the success of a social networking site, it is important that it engages the users by providing different services (Dhawan et al., 2014).

Despite the significant contribution of both privacy and security on social networking sites, it is necessary to determine the safety (Cheng et al., 2006). Prior studies pointed out that privacy is the most important issue for users when using the internet-based system because they might not be fully aware of the use of their online information; (Molla and Licker, 2001), while Chandio (2011) mentioned that security is important in Information technology. It can lead to a security threat, crime, loss of sensitive information and harm to reputation.

A study by Ahmad (2019), which studied Information Privacy Awareness among the Young Generation in Malaysia investigated the issues related to information privacy among the young generation in Malaysia and its implications of it. The findings of the study show that the young generation is vulnerable to privacy intrusion because they are really active on social media where a bunch of personal information reveals every day. And the study also recommended increasing the awareness of privacy, specifically for this young generation. Besides**,** another study by Zakaria et al. (2010) on The Use of Web 2.0 Technology by Malaysian Students' has revealed that the highest involvement with 2.0 Web applications is using the web to chat or instant messaging as well as social networking tools to socialize with friends and allowing others to access their profile from the web. Besides, it was also mentioned that this involvement shows how easily the information is exchanged from one hand to another in their daily activity. The findings highlighted on the lack of awareness of the privacy of Internet knowledge have increased the number of cases of Internet scams, online harassment, cross-site scripting and identity theft.

To elaborate, a study by Teong and Ang (2016) on Internet Use and Addiction among Students in Four Public Universities in East Malaysia found that extensively internet use can result in addiction, and the majority of the students' scores on internet addiction were rather high. Given that the majority of the students were exposed to the internet informally at a young age, and underline that these issues of internet usage pattern and addiction demand close attention. Additionally, it was noted that other countries have conducted a significant quantity of study on university students' internet usage patterns and internet addiction. Malaysian studies, meanwhile, are still quite few. Internet addiction has reportedly been associated with adverse effects such as misuse of social media (The Malaysian Times, 2013). Which is demonstrated in a study by Nor Hazlyna et al. (2021), who conducted a research on awareness about cyberbullying on social media among female students in public university of Northern Peninsular Malaysia. The study stated that students should be a priority population to focus on when discussing the problem of cyberbullying because this is a particularly important phase for identity building that can be difficult for them. The findings also demonstrated that when students are aware of cyberbullying, they can stop the incidence from happening. The existing studies (Nurhilyana et al., 2013; Haghighi et al., 2011; Hasmida et al., 2011) consistently reports that West Malaysian university students logged on their online platforms more frequently and spent a significant amount of time online. Focusing on this, the widespread use of social media among young people, particularly among university students, should demand urgent attention (Dongke & Sannusi, 2021).

Besides, Othman et. al (2013) conducted a study on privacy awareness in online social networks among undergraduate students to observe their usage purpose

and information disclosure. The findings stated privacy awareness in social network sites shows the majority of members are aware of the negative effect of using social networking sites. But significant minority users are not aware of the visibility of their profiles to others. It shows a different result in another study conducted by Acquisti and Gross (2006) which revealed that most users were unaware or oblivious to privacy-invading activities, as well as their risks, and had no idea of the extent to which their online were exposed for others to view. On social networking sites, users have the ability to control information about themselves and concerns about who can access and view their profiles. At the time they rely on themselves to control the flow of information by managing and addressing their privacy concerns. Despite these concerns, the study showed that users do not understand terms and policies clearly provided by the online social network service providers and it leads to misunderstanding of what information service providers share and release when users use social networking sites (Acquisti & Gross, 2006).

Sriratanaviriyakul et al. (2017) conducted a study about ASEAN users' privacy concerns and security in using online social networks and the result shows that ‘privacy’ correlates with ‘security’ but these two variables do not have a significant impact on users’ trust. Moreover, only ‘trust’ and ‘security’ affect users’ intention to use online social networks. In contrast, Shin (2010) conducted a study to develop a groundwork model of trust-based SNS acceptance to explain the factors contributing to the development of individual attitudes and behavioural intentions to use SNS. The finding shows that trust is affected by perceived privacy and perceived security which plays a role in the nature and effect of an individual’s attitude and behavioural intentions that a user performs with SNS communities. It could be recognized as the

significant role of privacy, security and trust as well as the major predictors of individuals' attitudes and behavioural intentions to use social networking sites.

The number of online users has been increasing rapidly which helps the fast growth of e-commerce and online transactions that motivate many companies to set up a business over the Internet (Meskaran, Ismail, & Shanmugam, 2013). The growth of online shopping in other Asian countries such as Malaysia is placed in the 'high rate' category (Meskaran et al., 2013). According to Hamid and Khatibi (2006), Malaysian, especially younger people were using the internet largely for activities such as seeking information, playing games, entertainment, or communicating with friends. The digital market communicates with consumers via social networks, by accessing online news and using search engines follows, (Nielsen, 2011). According to the research by Bhatt (2019) conducted on the Role of Security and Trust in Online Consumer Behavior to examine the impact of perceived trust, perceived security and privacy on the online purchase intention of the users. The result showed that Perceived trust has a positive impact on the online purchase intention of customers where trust is a key determinant of behavioral intentions. And highlighted that security should be considered the most important issue by the online sellers as it affects the customers' future purchase behavior. The online sellers' ability to protect privacy, security features and information shared by customers during their interaction with the website plays a vital role in the purchase process.

According to Jai and King (2016) on Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? The respondents for the study were individuals,

aged 18 years and older, who had made a purchase online in the previous six months. The results show that online shoppers significantly identified third-party advertisers and data brokers as separate agents and display different attitudes toward sharing their personal information in the context of online retailing. The study implies that age and gender also played important roles in predicting consumers' willingness to share their personal information with advertisers and data brokers.

Internet application use has been rising on the internet in recent years. E-commerce and social media platforms are at top of usage among all the internet sites. Bhatt (2019) revealed the role of security and trust in online consumer behavior on purchase intention and highlighted the importance of protecting privacy and security features while users share personal information on online platforms. Furthermore, several prior studies have also highlighted the issues of consumers' willingness to share personal information with online platforms & third-party advertisers, (Jai & King, 2016). More recently several studies have found the role of privacy and security in the development of trust in an e-commerce context, only a few studies have explored the topic in the SNS context. Social networking sites are mainly used for social interaction which has admitted significant research attention (Gupta & Dhami, 2015). Some prior studies have examined the user's acceptance of social networking sites with behavioral intention to use (JithiKrishna, Suresh Kumar & Sreejesh, 2015). Similarly, a study by Shin; (2010) also investigated the individual's privacy, security and trust, which affect users' attitudes and behavioral intentions to use social networking sites. In related social networking site research, some prior studies examined the social media usage purposes and information disclosure of students (Othman et. al, 2013). Interestingly, there is still limited research investigating the

role of privacy and awareness as an explanatory factors for users' willingness to share information on social- media sites (Paramarta et al., 2019). These issues are still very sensitive and under-researched areas, the harms caused by social media usage are relatively unknown (Willoughby & Mark, 2018). Despite previous studies, there is still lacking existing research on privacy, security and trust in information sharing that needs to be answered (Dhami, Agarwal, Chakraborty, Singh, & Minj, 2013).

Furthermore, the existing studies more focused on the internet based interaction and social media usage among public universities in East and Northern Peninsular Malaysia and however, the amount of time West Malaysian students spent on online platforms increased as they are very active on the platforms and get online more often (Nor Hazlyna, H et al., 2021; Teong and Ang, 2016; Nurhilyana et al., 2013; Haghighi et al. 2011; Hasmida et al., 2011). Whereas, in West Malaysia, Selangor is one of the most developed and highest population states with highest number of internet users such as social media active users in Malaysia (Lee & Mohamad, 2022; Department of Statistics Malaysia, 2021; Habibullah et al., 2018). Moreover, from public university students' can access high number of multicultural students, moreover, social media use by university students has emerged as an important research topic which need more focus and enhanced awareness among the academics (Rajan, Alam, Kia, & Subramaniam, 2021; Dongke & Sannusi, 2021).

Based on the aforementioned arguments, it is apparent that most studies in this field only focused on limited areas such as e-commerce, user behavior, user intention of using social media, issues & implications and online purchase intention and these researches were conducted in different countries and over a different group of people,

but there is a small number of researches for examining the effects of privacy, security and trust on information sharing in social media platforms. Besides, there is a limited researches evaluated in the social media context among the university students in Malaysia and more attention need at West Malaysia such as in Selangor due to the highest number of social media users. Thus, this research have been focused to investigate the effects of privacy awareness, security concerns and trust on information sharing in social media platforms among public university students in detail and realizing that it is extremely important to pursue this study to overcome the lacking of previous research.

1.4 Research Objective

RO1: To examine the effect of privacy awareness on trust toward social media sites.

RO2: To examine the effect of security concerns on trust toward social media sites.

RO3: To examine the effect of privacy awareness on information sharing on social media sites.

RO4: To examine the effect of security concerns on information sharing on social media sites.

RO5: To examine the effect of trust on information sharing on social media sites.

RO6: To examine the effect of privacy awareness on security concerns on social media sites.

1.5 Research Questions

To fill the gaps and achieved the research objectives, this study deals with the following questions:

RQ1: What is the effect of privacy awareness on trust toward social media sites?

RQ2: What is the effect of security concerns on trust toward social media sites?

RQ3: What is the effect of privacy awareness on information sharing on social media sites?

RQ4: What is the effect of security concerns on information sharing on social media sites?

RQ5: What is the effect of trust on information sharing on social media sites?

RQ6: What is the effect of privacy awareness on security concerns on social media sites?

1.6 Hypotheses of the Study

H1: Privacy awareness has a positive effect on trust toward social media sites.

H2: Security concerns have a positive effect on trust toward social media sites.

H3: Privacy awareness has a positive effect on information sharing on social media sites.

H4: Security concerns have a positive effect on information sharing on social media sites.

H5: Trust has a positive effect on information sharing on social media sites.

H6: Privacy awareness has a positive effect on security concerns on social media sites.

1.7 Theoretical Framework

The formulation of the research framework is guided by two major theories, namely Social Exchange Theory (SET) and Communication Privacy Management (CPM) theory.

Social Exchange Theory (SET) is based on the premise that human behavior or social interaction is an exchange of activity, tangible and intangible (Homans, 1961, p. 12-3), particularly of rewards and costs (Homans, 1961, p. 317-8). It treats the exchange of benefits, notably giving others something more valuable to them than is costly to the giver, and vice versa (Homans, 1961, p. 61-63), as the underlying basis or open secret of human behavior (Homans, 1961, p. 317) and so a phenomenon permeating all social life (Coleman, 1990, p. 37). Not only the market permeated by the exchange but also the non-economic realm, the social relations situated between extremes of intimacy, self-interest or cost-benefit calculation and disinterested, expressive behavior (Blau, 1964, p. 88-91).

According to Gouldner (1960), social exchange theory proposes that social behavior is the result of an exchange process. The purpose of this exchange is to maximize benefits and minimize costs. According to this theory, people weigh the potential benefits and risks of social relationships. When the risks outweigh the rewards, people will terminate or abandon that relationship (Surma, 2016). Besides, online social networks seem to be an ideal platform for social exchange because, they provide an opportunity to keep social relations at a relatively low cost compared to offline relations (Surma, 2016). According to Hall et al. (2010), social exchange

theory can be used as a way to describe the behaviors of information sharing online. In a previous study by Shin (2010), trust was highlighted as the most highly affected by security and privacy, and had a strong impact on the users' intention to share information on social media platforms. In order to better understand people's willingness to share information in exchange for personalized benefits, social exchange theory provides a useful conceptual framework (Martin & Murphy, 2017). Numerous studies employ various social exchange theory derived constructs into their models. In one investigation, proposes a research model to examine the relationships among SET-based variables and the study highlighted the key social exchange issues which are trust and information sharing in their study (Wu et al., 2014). Similarly, study by Cloarec, Meyer-Waarden, and Munzel (2022) highlighted that the degree to which internet satisfaction influences the personalization-privacy issues, where they focuses on the social exchange theory based constructs of trust and willingness of information sharing. Besides, another study by Dhami et al., (2013) investigated the research model using social exchange theory based variables which shows that perceived privacy and perceived security are antecedents of perceived trust and trust strongly impacted by privacy and security as well as, privacy and security have positive effect on information sharing. Hence, in this research, the social exchange theory (SET) has been used as the theoretical framework because the individual's information sharing on social media is an exchange between individuals and social media platforms. Thus SET provides an analytically tested frame for exploring the key factors of the relationships between variables and their effects on the normative aspects of exchange that affect information sharing willingness, particularly: privacy awareness, security concerns and trust of social media users.

The second theory is Communication Privacy Management (CPM) theory which defines private information as something a person owns (Petronio & Caughlin, 2006). According to Baxter et al. (2014), the boundaries of individual ownership regarding personal data are defined by communication privacy management theory using a boundary metaphor and boundaries highlight the transactional aspect of how that information is maintained with others. Additionally, CPM defines personal information as people who think they are in control of their personal information and can make decisions about it if they are aware that there could be potential breaches.

According to Petronio (2002), Building metaphorical barriers is a method used by the theory of CPM to explain how people maintain their personal information. As Cavusoglu, Phan and Airoldi (2016) stated, the theory of communication privacy management describes how people can manage disclosures by way of restriction measures to ensure a proper balance between accessibility and secrecy. The CPM theory also explains how users manage their own privacy in various communication contexts using different social media platforms (Petronio, 2002; 2013). According to Zlatolas et al. (2019), communication privacy management can be defined as the process of opening up and closing borders to others.

Most applications of the communication privacy management theory are in the areas of community, interpersonal, and clinical communication (Petronio & Durham, 2014). Zlatolas et al. (2019) refers that the area of social media, privacy research has received the greatest attention. Besides, it is highlighted in a study by Choi et al. (2011) that, the communication privacy management theory primarily examines the privacy vulnerabilities related to social media. According to the communication

privacy management theory, privacy ensures that people control which data they disclose and to whom by employing social media privacy controls that are similar in concept to offline interaction (James et al., 2015; Petronio, 2002). It is expected that communication management theory is applicable to assessing users' social media usage patterns since online users will decide about ownership of the data, controls, and set the boundaries for their personal information. At the same time, communication privacy management theory aligns well with social media sites since users may choose who they share their information with on these platforms. Also communication privacy management theory used more as the basic theory behind previous study model on privacy and information disclosure (Zlatolas, Hrgarek, Welzer, & Hölbl, 2022). Hence, in this research, the CPM theory is included to examine the users' privacy management of their personal information sharing on social media. This study intends to explain the relationship between several CPM-derived variables (Widjaja, Chen, Sukoco, & Ha, 2019; Zlatolas, Welzer, Hölbl, & Heriˇ, 2019; Zlatolas, Welzer, Heričko, & Hölbl, 2015) privacy awareness, trust and social media users' willingness to share information on social media sites .

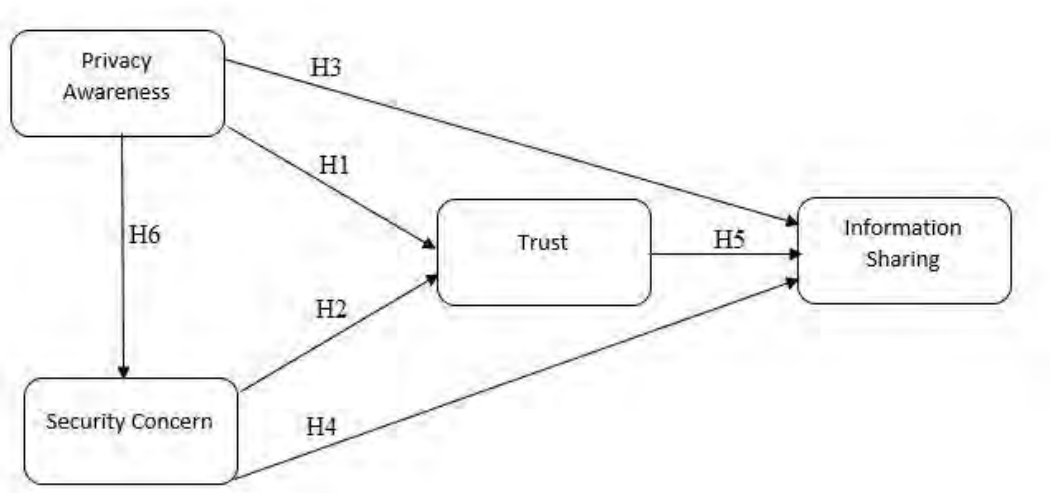

Figure 1.1. Proposed conceptual framework

1.8 Operational definition

1.8.1 Privacy Awareness

According to Malhotra et al., (2004), the level of knowledge about information privacy measures is referred to as privacy awareness. On the other hand, Zlatolas et al. (2015), explained that privacy awareness refers to how much a person is notified about privacy practices. Furthermore, individuals' awareness to their privacy of potential dangers and threats on social media sites that could have negative effects, cause harm and something loss in result (Koohang & Georgia, 2021).

Thus, in this study, privacy awareness will be referred to as how much the students are aware about the potential dangers or threat and notified about privacy practices on social media sites.

1.8.2 Security Concerns

Security concerns can be defined as the beliefs of individuals about the risks and potential negative effects of information sharing (Baruh et al., 2017; Zhou & Li, 2014; Cho et al., 2010).

However, according to Zhang & Gupta (2016), security concerns definition is that individual's concerns about the safety of their private details against stealing the personal data on social media platforms (attackers collecting individual's data without their knowing); impersonation/social phishing (aggressors mimicking a genuine

individual through a fake site to take information, login accreditations, Mastercard numbers) and other security issues on social media sites such as, hijacking (where attackers take over a target's profile); picture retrieval/analysis (where assailants utilize confront-and picture-recognition computer program to learn more approximately targets and the related profiles they are related to and malware attacks, in which an attacker sends malicious scripts or software to individuals' gadgets to carry out actions without their understanding. Thus, in this study, security concerns will be assigned to the concerns of students' about their safety and how secure their personal information on online platforms.

1.8.3 Trust

According to Shin (2010), social media platform represents a virtual community in which people with shared interests can communicate by posting and exchanging information about themselves.

According to Rousseau et al. (1998), trust is defined as the willingness to accept a vulnerable situation based on a positive expectation regarding the actions of others. Besides, trust refers as the degree to which someone is willing to rely on social media platform (Lankton & Tripp, 2013). Moreover, according to Dhami et al., (2013), a person's acceptance of a social media site's capacity to protect personal information is referred to as trust. Therefore, in this study, trust will be referred as the students' belief of revealing information and performing any task on social media platforms is risk-free.

1.8.4 Information Sharing

Information sharing can be defined as the voluntary act of making information held by one entity available to another entity. As a result, information sharing is crucial for meeting the requirements of others in terms of making socioeconomic decisions (Masele, 2022). In another words, information sharing can be defined as providing details to others and getting information that has been offered by the information sender which are the two main components of the process of information sharing (Savolainen, 2017).

According to Paramarta et al. (2019), information sharing is an individual's belief that they will share personal information on social media platforms. Thus, in this study, information sharing will be referred as the university students' belief that they will share their personal details over social media platforms.

1.9 Importance of the Study

This study aims to identify the effects of university students' privacy awareness, security concerns and trust while their personal information sharing on social media platforms. The outcomes are intended at helping and providing a better understanding to the university students about their privacy, security issues and trust while sharing their personal information on social media platforms. Besides the university students, this study can be also helpful for other groups of the population as well as the social media service providers.

1.10 Limitations of the study

This study focuses on the university students' privacy awareness, security concerns and trust in information sharing on social media platforms. This study has constraints and limitations that need to be addressed in the implementation of the study. The limitations faced in carrying out this research are that this research is focused only on university students, and the data collection by respondents is limited to the Public Universities in Selangor, Malaysia only. In addition, the results obtained through the implementation of this study do not reflect the whole population but only provide a picture of the sample selected for this research.

1.11 Research Structure

This research is divided into five chapters. Chapter 1 introduces the issues related to the topic under the investigation and explains the basic ideas of the research, and research objectives, considers significant constructs to be included in the proposed framework and discuss hypotheses to be tested. Chapter 2 critically review the relevant literature pertaining to privacy, security, and trust on information sharing on social media. Chapter 3 describe the research methodology adopted to test the proposed hypotheses. Chapter 4 presents and interprets the empirical results drawn from hypothesis testing. Chapter 5 discusses the main findings of the research; points out the research implications and limitations, as well as provides recommendations for future research and draws a conclusion.

1.12 Summary

This chapter discussed the overview of research on the effects of privacy awareness, security concerns and trust on sharing information on social media among students. In this part, a brief introduction was explained on the issues of privacy awareness, security concerns and trust on sharing information on social media. In addition, this research has been conducted to provide a better insight into privacy and security as well as a few research in the field of privacy and security are also included and discussed in the problem statement. The problem statements are the main questions that need to be answered at the end of the research. The research objectives have been specified and followed by the research questions. Hypotheses statement also has been made in the introduction section as well as the operational definitions also have been discussed in this section. In the next chapter, the relevant literature referring to privacy awareness, security concerns and trust on sharing information are to be critically reviewed.