The Effects of Privacy Awareness, Security Concerns and Trust on Information Sharing in Social Media among Public University Students in Selangor

Anjuman Ara[a]*, Zuraidah Zainol[b], Balaganesh Duraisamy[c]

[a, b] *Faculty of Management & Economics, Sultan Idris Education University, Malaysia*
[c] *Faculty of Computer Science and Multimedia, Berlin School of Business & Innovation, Germany*
[c]*Faculty of Computer Science and Multimedia, Lincoln University Collage, Malaysia*
Corresponding Author: aranjuman1306@gmail.com

To cite this article (APA): Anjuman Ara, Zuraidah Zainol, & Duraisamy, B. (2022). The Effects of Privacy Awareness, Security Concerns and Trust on Information Sharing in Social Media among Public University Students in Selangor. *International Business Education Journal*, *15*(2), 93–110. https://doi.org/10.37134/ibej.Vol15.2.8.2022

To link to this article: https://doi.org/10.37134/ibej.Vol15.2.8.2022

Abstract

The purpose of this research was to investigate the effect of privacy awareness on security concerns, privacy awareness and security concerns on trust, and privacy awareness, security concerns and trust on information sharing in social media platforms. This research employed a quantitative method. Data were collected from a sample of 500 public university students, in the age range of 18-29 years old. Data were collected using a questionnaire as an instrument and the selection of respondents was made using the systematic street-intercept method. Covariance-based Structural Equation Modeling (CB-SEM) was used to analysed the obtained data. The findings revealed that privacy awareness (PA) significantly predicts security concerns (SC). Both PA and SC turn out to be significant predictors of trust. However, the effect of PA is positive, while SC is negative. Only PA and trust significantly affect the information sharing (IS), not SC. Trust is more likely to increase the willingness to share information, but the higher the SC, the less likely for the students to share information. In conclusion, to promote IS on social media platforms, trust should be built among the users. Despite that privacy awareness could reduce the willingness to share information, it plays a critical role to build trust. In implication, to win and secure the online users, the online service providers and sellers should overcome the trust and privacy issues.

Keywords

Privacy Awareness; Security Concerns; Trust; Information Sharing.

INTRODUCTION

Social media is an important tool and easy path for everyone to communicate and exchange information with each other and yet, it exposes the users especially young individuals to the risk of online data privacy and security including data misuse, scams, and cyber-bullying (Nurul Madiha & Mohd Azul, 2015; Vemprala & Dietrich, 2019; Willoughby and Mark, 2018; Yuen Meikeng & Clarissa Say, 2018). The global social media penetration rate was reported to be around 49 per cent, East Asia was ranked first with a penetration rate of 71 per cent (Clement, 2020), and Southeast Asia's maximum social penetration rate was in Malaysia, which was listed in the top five countries worldwide (Bernama, 2019), highlighting Malaysia as being in a very risky position to deal with privacy issues and being the top five target for cybercrime (Haris, Sarijan, & Hussin, 2017; Reddy & Reddy, 2019; Yuen Meikeng et al. 2018).

Manuscript received Sept 22, 2022; revised Nov 1, 2022; published Dec 20, 2022

Hence, to avoid becoming a victim of a personal data breach, it is important for social media users to must be concerned of the dangers of personal information sharing on platforms for social networking and make the right decision to disclose personal information only when needed. That is, it is crucial to understand what drives individuals to share information.

To date, many studies examining this phenomenon, but there is still a lack of clear understanding of why individuals disclose despite privacy and security concerns remain (Kolotylo-Kulkarni, Xia & Dhillon, 2021). Despite extensive empirical evidence on perceived privacy, security, and trust on social media, most of the studies tend to link with social media usage (JithiKrishna, et. al, 2015; Sriratanaviriyakul, et al 2017) or issues of e-commerce context (Jai & King, 2016) as the ultimate outcome. Few studies have performed to investigate into the impact of perceived privacy, security, and trust on desire to disclosure of information (Kolotylo-Kulkarni et al., 2021). It is; therefore, this research seeks 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 social media platform.

LITERATURE REVIEW

Theoretical Framework

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

According to Social Exchange Theory (SET), the main purpose of it to maximize better benefits and reduce costs and this social behavior is the outcome of an exchange process (Gouldner, 1960; Homans, 1961). That is, people would then consider the potential rewards and pitfalls of the forming social connections. Individuals have a higher tendency to continue the connection when the benefits exceed the hazards, and put an end when the risks outweigh the rewards (Surma, 2016). Social exchange does occur on the online platform (Hall, et al. 2010). Comparing online and offline relationships, the platform of social networking sites offer people the chance to maintain social connections at low-cost which appear to be the appropriate site for social exchange (Surma, 2016). In deciding to share or not to share the information online, people also gauge the derived benefits of such sharing (Hall, et al. 2010). That is, whenever the benefits gained are greater than the costs incurred, individuals are more willing to disclose their private details.

On the other hand, Communication privacy management (CPM) theory asserts that individuals have specific rules in the decision made to disclose and protect private information (Sandra Petronio & Rachael Hernandez, 2019). As per CPM theory, people truly believe that they own their personal information, hence they have the power to govern it (Petronio, 2004). People set limits to preserve the information they consider private since disclosing private information to others would pose a certain level of risk. By setting privacy rule boundaries, people can maintain the balance between their desire for privacy and the necessity of disclosing particular private information (Kisekka, Bagchi-Sen, & Raghav Rao, 2013). Hence, in deciding whether to share personal data on social media, individuals would create security and privacy preferences that they later use in order to either keep out of sight or expose their personal information (Kisekka, et al. 2013).

Accordingly, the theories suggest that in understanding the wiliness to share personal information, it is critical to understand how individuals set the boundaries on privacy, security, and trust issues, in which individuals are more possibly to share the information if all the boundaries are resolved.

Explication of Constructs

According to Zlatolas, Welzer, Heričko, and Hölbl (2015), the degree to which users are informed about privacy issues, infractions, and policies on social networking sites is known as privacy awareness while Padyab, Päivärinta, Ståhlbröst and Bergvall-kåreborn (2019) define it as the level of users' consciousness of privacy issues and violations, and also with social media-related privacy practices. Similarly, Ampong et al. (2018) relate privacy awareness to the knowledge of people and their perception of the privacy options accessible on social media. Accordingly, in this research, privacy awareness is referred to as how much the respondents are notified about the online privacy practices.

Security concerns refers to individual's concerns about the safety of their private details against stealing the personal data on social media platforms, in which users who are really concerned about security problems can configure different security settings in social networking application including restricting viewers from looking at their personal information (Joe, 2014; Zhang & Gupta, 2016). Besides, security concerns can be defined as the beliefs of individuals regarding the hazards and possible negative effects of information disclosure (Baruh et al., 2017; Zhou & Li, 2014; Cho et al., 2010). Thus, in this research, security concerns are regarded as the beliefs that the respondents hold about the risks and possible negative effects of online information sharing.

According to Gefen's definition from 2002, trust is the ability to make yourself vulnerable to the actions taken by the reliable party based on a sense of confidence or assurance. Grazioli and Jarvenpaa (2000) refer to trust as people's belief that others will act according to people's expectations, while Dhami, et al., (2013) define trust as a person's belief in the social media platform capability that is risk-free to share information or execute any function. Therefore, in this research, trust is meant as the respondents' faith that sharing information also performing any task on social media platforms is risk-free.

Information sharing can be defined as providing details to others and getting information that has been offered by the information sender are the two main components of the process of information sharing (Savolainen, 2017). According to Paramarta et al. (2019), a person's intention to disclose personal information on a platform for social netwroking is known as information sharing. On the other side, information sharing which can be defined as the voluntary act of making information held by one entity available to another entity (Masele, 2022). Thus, in this research, information sharing refers to the willingness of students' to make their information available to another entity over a social media platform.

Hypothesis Development

A study involving Facebook users also disclosed that an increased level of awareness regarding privacy issues lead to improved trust in the service providers and for that they are willing to share even more about themselves on the platform (O'Bien & Torres, 2012; Hoadley et al., 2010). Paramarta (2019) also showed that increased awareness of privacy is more likely to increase a user's trust level. Even Saleh et al. (2016) that studied the youngsters, demonstrated that users' awareness of privacy is positively associated with trust. Gupta and Dhami (2015)

showed that there is a positive relationship between perceived privacy and perceived trust, suggesting that users' trust level rises when they are given enhanced security when accessing their profiles.

In addition, Paramarta et al. (2019) showed that increased security will increase a user's trust level, while Shin (2010) highlighted that trust is significantly impacted by both security and privacy. That is, the improved feelings of privacy and security would lead to an improved perception of trust. Therefore, it could be expected, privacy awareness and security concerns will significantly affect the trust. Hence, in this research, it is hypothesized that:

H1: Privacy awareness has a significant effect on trust toward social media sites.
H2: Security concerns have a significant effect on trust toward social media sites.

Users who possess high privacy awareness tend to maximize the privacy features that have been provided by platform for social networking, to protect information about them, which may result in more careful behaviour whenever they are engaged online (Paramarta, et al., 2019; Tuunainen, et al. 2009). Zlatolas et al. (2015) found a negative outcome of privacy awareness on information sharing, indicating that users will be less willing to disclose information as a result of increased awareness about privacy issues. However, other studies revealed that an individual who is knowledgeable about privacy issues tends to have control over their privacy which consequently increases the readiness to share personal details via social networking sites (Padyab, et al. 2019; Paramarta, et al., 2019). It was also highlighted that social media users that have high individualism are more concerned about potential privacy interruption and seem to be quite willing to keep their personal information safe, which leads to share less of their personal information online (Cho et al., 2009). As a consequence, it could be expected of a significant effect of privacy awareness on willingness to share information on social media. Hence, it could be hypothesized that:

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

Almadhoun, Dominic and Woon (2011) showed that a security guarantee does not make the users feel safe and secure to share sensitive information about themselves over the SNSs and that they are reluctant to share their personal data. Nevertheless, Gupta and Dhami (2015) demonstrated that users' interest in sharing information on social media platform such as Facebook grows if they are given higher level of internet security. Along a similar line, Kayes, Kourtellis, Bonchi and Iamnitchi (2015) revealed that enabled security settings are more likely to induce the users to engage more in the online platform and share information, while Paramarta et al. (2019) showed that if an individual has authority over the social media platform's security settings, their willingness to disclose information on social media might increase as they feel secure. Thus, it could be believed that security concerns have a significant effect on the willingness to share information on the online platform. Hence, it is hypothesized that:

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

Users' trust in social media sites is a vital determinant of information sharing (Shin, 2010). However, the direction of the impact is rather varied. On one hand, it was stated that despite higher-level trust on the site, the users will not be encouraged to post personal information on social networking sites (McKnight, D.H., Lankton, N. & Tripp, J., 2011).

However, a study by Taddei, et al. (2013) clearly showed, the stronger trust on the social media site, the higher the preference for users to share information. Dhami et al. (2013) also identified a positive connection between users' trust and the intention of users to share information. Similarly, Gupta and Dhami (2015) showed users' trust will raise their readiness to share information. Accordingly, it could be expected the significant effect of trust on information sharing. Henceforth, the current research developed the following hypothesis:

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

Perceived privacy is often confused with perceived security, and used interchangeably in many past studies (Shin, 2010). In particular, perceived privacy relates to the awareness of how personal information should be handled online such as which dare is typically revealed a profile is created, where personal data will be stored, how data will be used and the possibilities of privacy breaching, while security concerns refer how users perceived the technological practices and approaches used by online social networking providers to assure that the personal details of users is managed effectively as well as free from risk (Flavián & Guinalíu, 2006). In past studies, the relationship between these two variables has been established. Specifically, in developing a model for the acceptance of SNSs based on trust, Shin (2010) revealed the positive effect of perceived privacy on perceived security. Along a similar line, Sriratanaviriyakul et al. (2017) showed that privacy has a positive significant impact on security. Thus, based on the above arguments, it could be expected of a significant effect of privacy awareness on security concerns. Therefore, it could be hypothesized that:

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

Figure 1 depicts the hypothesized relationships to be tested in this research.

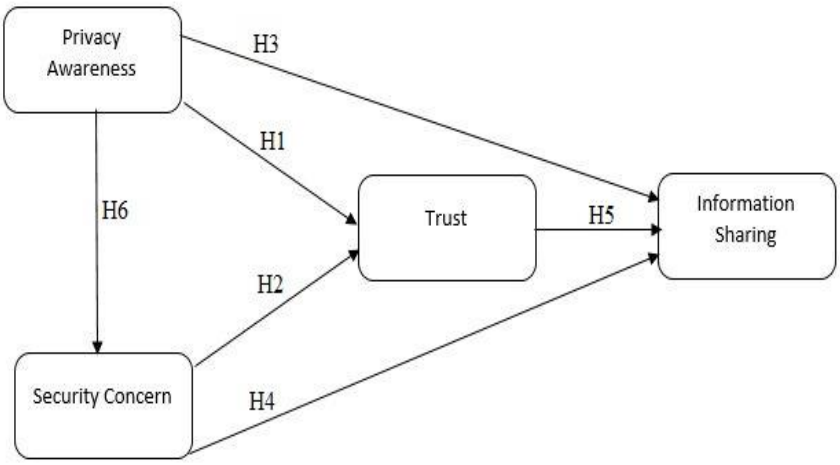

Figure 1: Proposed conceptual framework (Source: Developed for the research)

METHODOLOGY

The research aims to produce empirical evidence on the roles of privacy awareness, security concerns as well as trust in influencing the tendency to share information on online media sites. Hence, this research adopted a quantitative approach, the most appropriate method to quantify

the data and conclusive evidence which is based on representative samples (Malhotra, 2002). This research has been done in Selangor which is considered the Malaysian state with highest percentage of internet users (Malaysian Communications and Multimedia Commission, 2017). The unit used for this analysis is individual.

The population of this research is social media users in Selangor, Malaysia. Given that younger adults in the age range of 18 to 29 years old have the highest likelihood to use social media (Perrin, 2015), the sample of this research was composed of social media users aged from 18 - 29 years old. Since most of the social media users between the age ranges of 18 to 29 can be found in universities, this research took place in four public universities in Selangor. To select the sample, a systematic random sampling technique was used. Specifically, every tenth student that enter the main entrance of the universities was chosen as the sample.

Based on a total number of 264,820 students at four public universities in Selangor (Ministry of Education, 2019), 384 is suggested for minimum size of sample to represent its population (Krejcie and Morgan, 1970). However, considering the requirement to meet the recommended size of the sample for conducting data analysis of structural equation modelling (SEM) (Hair et al. 2012), the nonresponse and other constraints, the addition of 30% was made to the sample size (Fairbairn & Kessler, 2015). Accordingly, 500 was set as the adequate sample size for this research.

For data collection, a set of questionnaire was used as an instrument. The questionnaire was divided into two parts, Part A contains items to measure the constructs such as privacy awareness, security concerns, trust, and information sharing, while Part B is comprised of demographic questions. All the items in Part A were adapted from past research. In particular, items to measure privacy awareness were adapted from Ampong et al. (2018), Zlatolas, Welzer, Heričko and Hölbl (2015) and Krasnova, H. et al. (2010), and security concerns from Tuunainen, Pitkänen and Hovi (2009), Dinev, T. Hart, P (2006), and Zlatolas, Welzer, Heričko and Hölbl (2015), trust from Fogel and Nehmad (2009), and Dwyer, Roxanne Hiltz, Passerini, and Roxanne (2007), and information sharing from Zlatolas et al. (2015), Aljohani, Nisbet, and Blincoe (2016) and Beldad (2015).

To revise the questionnaire and validate the measurement items, two pilot tests were conducted involving two groups of people i.e., the experts and the potential respondents (Saunders et al. 2009). The experts consisted of a panel of two academicians that hold a PhD in Business Information Systems and Industrial Technology Management at Sultan Idris Education University. Based on the experts' feedback, several items were reworded, and instructions were simplified. Next, a pilot study was also conducted with 100 respondents as suggested by Hertzog (2008) for several improvements like clarity, validity, and reliability of the questionnaire. Specifically, the validity is achieved through the exploratory factor analysis (EFA) with a Kaiser-Meyer-Olkin (KMO) test of 0.764, significant Bartlett's Sphericity test value and total variance explained of 56.52, while reliability is achieved when the Cronbach's alpha values were all above 0.7.

Due to the Covid-19 pandemic, the data collection process took about 13 months to complete, i.e., from February 2021 to February 2022 at the universities. Participation of the respondents was voluntary and anonymous, and all the data obtained were treated with strict confidentiality. Covariance-based Structural Equation Modeling (CB-SEM) was used to test the hypotheses.

RESULTS

Profile of Respondents

Based on Table 1, a total of 401 questionnaires were generally returned where the number of distributed questionnaire was 500, which represented a response rate of 80.2%. However, 28 responses were incomplete with more than 10% of the items left unanswered (Hair, et al., 2010). Hence, the 28 responses were excluded, and the remaining 373 responses (valid response rate of 74.6%) have been used for further data analysis. The highest number of the respondents were female (72.4%) and Muslim (78%), along with average age of 22.28 years old. Bachelor's degree students were reported the highest participated respondents with a percentage of 61.1% and followed by the Postgraduate degree students with the percentage of 21.2%. Most of the respondents spent more than 3 hours a day on social media (52.3%) and prefer Instagram (42.6%), over Facebook (28.7%), Twitter (21.2%) and other platforms (7.0%).

Table 1: Respondents' Profile

		Frequency	Per cent	Mean	Std. Deviation
Gender	Male	103	27.6		
	Female	270	72.4		
Religion	Islam	291	78.0		
	Buddha	34	9.1		
	Hindu	15	4.0		
	Christian	24	6.4		
	Other	4	1.0		
Age	18 years	5	1.3	22.28	2.963
	19 years	57	15.3		
	20 years	78	20.9		
	21 years	48	12.9		
	22 years	46	12.3		
	23 years	27	7.2		
	24 years	22	5.9		
	25 years	25	6.7		
	26 years	18	4.8		
	27 years	17	4.6		
	28 years	14	3.8		
	29 years	16	4.3		
Education	Diploma/ Certificate	66	17.7	3.03	0.623
	Bachelor's degree	228	61.1		
	Postgraduate degree	79	21.2		
Time spent on social media (per day)	One hour	42	11.3	3.13	1.062
	Two hours	63	16.9		
	Three hours	73	19.6		
	More than three hours	195	52.3		
Preference social media platform	Facebook	107	28.7	1.92	0.731
	Instagram	159	42.6		
	Twitter	79	21.2		
	Other	26	7.0		

Preliminary Analysis

Examination of the missing values reveals no missing values, indicating that no responses should be excluded. Inspection of the skewness and kurtosis results found that there's no values beyond the threshold of ±2 (Garson, 2012a), satisfying the univariate normality. However, the Mardia's coefficient of multivariate kurtosis shows a value of 144.061 with the critical ratio of 44.759, which is excessively high than the acceptable point of not exceeding 1.96 (Garson, 2012a), implying multivariate non-normality.

As to reduce the multivariate nonnormality, deletion of extreme outliers is required. Hence, an inspection of standardized z scores (thresholds of ±4) and Mahalanobis distance (threshold of p1<0.001) was conducted. Since no values exceeded ±4, there are no univariate outliers (Hair et al., 2010), but Mahalanobis distance reveals 37 extreme cases, which need to be deleted (Kline 2011). The deletion of 37 observations merely causes about 7.4 per cent of data loss but improves the multivariate non-normality. Despite the nonnormality, since the extreme non-normality has been reduced, the available data are an acceptable representative of the general population (Gao et al., 2008). Hence, the remaining data of 336 are used for further analysis. Furthermore, the inter-construct correlations and factor loadings are all below 0.9, which indicates no multicollinearity issues (Garson 2012a; Hair et al. 2010).

The possibility of common method bias exists when collecting cross-sectional data from a single informant using the same questionnaire (Bhattacherjee 2012; Cater & Cater 2010; Podsakoff et al. 2003). Thus, to check on the bias, Harman's single-factor method was used (Podsakoff et al. 2012). Exploratory factor analysis was performed which shows that a single factor solution only explains 24.929 per cent of the variance (Table 2), indicating the nonexistence of common method bias (Gaskin 2012b; Podsakoff et al. 2003).

Table 2: Harman's Single-factor Test (EFA Results)

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.235	24.929	24.929	5.235	24.929	24.929

Using the confirmatory factor analysis (CFA), the single model shows a poor fit compared to the proposed model (Table 3), which assures the nonexistence of common method bias (Zaefarian et al. 2013).

Table 3: Comparing Model Fit Indices

Goodness-of-fit Statistics	**Harman's single-factor Model**	**Proposed Model**	**AcceptableValue***
χ^2(df, p)	2237.060 (209, 0.000)	465.528 (183, 0.000)	Significant
χ^2 /df	10.704	2.544	1 to 5
CFI	0.254	0.896	> 0.9
TLI	0.251	0.881	> 0.9
RMSEA	0.170	0.068	< 0.08

* Acceptable values are based on Schumacker & Lomax (2004), Reisinger & Mavondo (2007), Hair et al. (2010), Garson (2012a), Gaskin (2012b) and Bagozzi & Yi (2012)

The Measurement Model's Validation

The measurement model fit is determined using this research analysed by $\chi 2$, normed $\chi 2$, comparative fit index (CFI), Trucker-Lewis index (TLI), Goodness of fit index (GFI), root mean square error of approximation (RMSEA), and standardized root means square residual (SRMR) are still below the considered acceptable levels of a model fit. According to Table 4, the initial model fails to achieve the acceptable fit. To improve the goodness-of-fit (GOF), the standardized regression weight (factor loading), standardized residual covariance matrix and modification indices were evaluated. The GOF is only achieved with the deletion of two items (PA8 and IS3) due to low loading and correlating the e9 and e10 due to high modification indices.

Table 4: Goodness-of-fit (GOF) Indices

GOF statistics	$\chi 2$ (df,p)	$\chi 2$/df	CFI	TLI	GFI	RMSEA	SRMR
Acceptable value*	Significant at $\alpha = 0.05$	1-5	> 0.9	> 0.9	> 0.9	< 0.08	< 0.08
Initial GOF	465.528 (183, 0.000)	2.544	**0.896**	**0.881**	**0.880**	0.068	0.0681
Final GOF	318.094 (145, 0.000)	2.194	0.933	0.921	0.906	0.060	0.0574

* based on Schumacker & Lomax (2004), Hair et al. (2010) and Garson (2012a)

Once the GOF is achieved, the measurement model's reliability and validity are checked. Refer to Table 5 for results. The construct reliability ranges from 0.720 to 0.883, establishing the internal consistency with values above 0.7. To confirm the convergent validity, the standardized factor loadings and average variance extracted (AVE) were examined. The AVE values for PA and T are more than the criterion of 0.5, while AVE for SC and IS are below the cutoff of 0.5 (Hair et al., 2010). Since the AVE that is less than 0.5 is considered acceptable as long as the construct reliability is greater than 0.6 (Fornell and Larcker, 1981), the convergent validity is considered satisfied. What is more, the convergent validity is established as the standardized factor loadings for all constructs greater than 0.5. Next, the discriminant validity was examined by comparing the square root of the AVE with the corresponding inter-construct correlations (IC). The results show that the square root AVE for all constructs is larger than their IC, establishing the discriminant validity (Ramayah et al. 2010; Chiu & Wang 2008; Fornell & Larcker 1981).

Table 5: Evaluation of the Measurement Model Inter-construct

	Convergent Validity			Discriminant Validity			
Constructs	**CR**	**AVE**	**MSV**	**PA**	**SC**	**T**	**IS**
PA	0.883	0.653	0.151	**0.808**			
SC	0.866	0.449	0.151	0.389	**0.670**		
T	0.821	0.605	0.154	0.144	-0.128	**0.778**	
IS	0.720	0.393	0.154	-0.280	-0.196	0.392	**0.627**

Note:
AVE = average variance extracted = Σ squared loadings/n,
CR = construct reliability = (Σ loading)2/[(Σ loading)2 + Σ (1-factor loading2]
*** denotes a significant at $p < 0.001$, MSV represents maximum shared variance.

Hypotheses Testing

As depicted in Table 6 and Figure 2, goodness-of-fit (GOF) for the structural model is achieved, i.e., significant χ^2=279.914 (df=128, p=0.000), χ2/df=2.187 is below 5, CFI=0.937, GFI=0.913 and TLI=0.924 are above 0.9 and, RMSEA=0.060 and SRMR=0.0558 is lower than 0.08.

For the first equation, the R^2 is 0.06, indicating that 6.0 per cent of the variation in trust can be explained by privacy awareness (PA), and security concerns (SC). Further, at the significance level of 0.05, both the PA and SC have a statistically significant effect on trust (p-value < α), in which PA has a positive effect on trust (β=0.273, p<α), while SC has a negative effect on trust (β=-0.227, p<α). Hence, the higher the PA, the higher the trust in the platform for social networking and vice versa, but the higher the SC, the lower the trust in the social media platform and vice versa. Thus, both H1 and H2 are supported.

As for the second equation, the R^2 value shows that 27.0 per cent of the variation in information sharing (IS) is explained by privacy awareness (PA), security concerns (SC) and trust (T). In particular, the PA has a significant negative effect on IS (β =-0.400, p<0.05), SC does not have a significant effect on IS (β=-0.020, p>0.05), and trust has a significant positive effect on IS (β=0.447, p<0.05). Hence, H3 and H5 are supported but not H4. The findings imply that the higher level of PA, the less likely for students to share information on the social media platform, but a higher level of trust on social media platforms is more likely to increase the willingness to share information on social media.

Finally, the outcomes show that 17 per cent of the variation in SC is explained by PA. specifically, PA significantly and positively affects SC (β=0.464, p<0.001). Thus, H6 is supported. Accordingly, the outcomes indicate that the higher level of PA, the more likely the student is to be concerned about the security aspects of social media platforms.

Table 6: Summary of the Hypotheses Testing

Hypotheses	Hypothesized path	Standardized estimation	P-value	Result
R^2 (T) = 0.06				
H1	PA → T	0.273	0.001	Supported
H2	SC → T	-0.227	0.003	Supported
R^2 (IS) = 0.27				
H3	PA → IS	-0.400	0.000	Supported
H4	SC → IS	-0.020	0.796	Not supported
H5	T → IS	0.447	0.000	Supported
R^2 (SC) = 0.17				
H6	PA → SC	0.464	0.000	Supported

Note:
IS - information sharing, PA -privacy awareness, SC - security concerns, T - trust

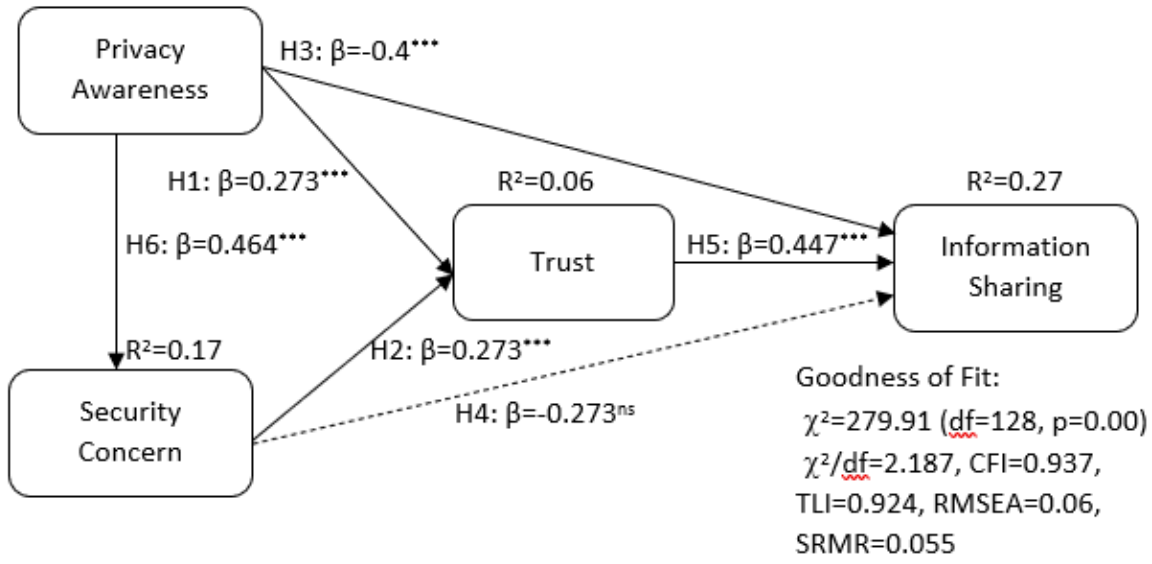

Figure 2: The Proposed Structural Model's Test Results

DISCUSSION AND CONCLUSION

Overall, five out of six hypothesized relationships are supported. In particular, it is supported that students' privacy awareness would increase their concerns with the security aspects of the social media platform, and both the privacy awareness and security concerns will significantly impact the level of trust towards social media. While privacy awareness increases the trust level, security concerns decrease the trust level. Privacy awareness along with trust influence the users willingness to share personal information on social media, in which privacy awareness is less likely to induce the willingness, but a higher level of trust is more likely to increase the willingness to share information. As for the security concerns, it has no significant effect on the willingness to share personal information.

Hence, the findings support the previous findings on the positive effect of perceived privacy on perceived security (Shin, 2010; Sriratanaviriyakul et al., 2017). That is, the higher the understanding and awareness of the online privacy aspects, the users tend to view the security issues of social media more favourably.

Besides, the findings support the past findings on the significant effect of privacy awareness and security concerns on trust. That is, the findings concur with past studies on the positive effect of privacy awareness on trust (Gupta & Dhami, 2015; Hoadley et al., 2010; O'Bien & Torres, 2012; Paramarta, 2019; Saleh et al., 2016), in which higher level of awareness about privacy issues is possibly to increase the trust level in the social media service providers.

However, the findings partially supported the past studies on the effect of security concerns on trust. While past studies revealed the positive effect of security concerns on trust (Paramarta et al., 2019; Shin, 2010), the results of the present study reveal the opposite. That is, the more favourable perception that the users have about the security of the social networks, the less likely for the users to put trust over the online media platforms. It may be that the

security aspect that social media has made publicly fails to convince users of the ability of social media to guarantee the safety of users so that they do not place high trust.

With respect to the willingness to share information online, the findings support the past studies that the more the users are informed about privacy, the less they want to share their personal details on social media (Cho et al., 2009; Zlatolas et al., 2015), but the stronger trust on the social media site, the higher the preference for users to share information (Gupta & Dhami, 2015; Singh et al., 2013; Taddei, et al., 2013). As for the security concerns, the findings refute the past studies (Gupta & Dhami, 2015; Kayes, Kourtellis, Bonchi & Iamnitchi, 2015; Paramarta et al., 2019) by pointing out the insignificant effect on the willingness to share information. That is, a security guarantee does not seem to make the users feel totally safe and secure in sharing sensitive information about themselves (Almadhoun, Dominic & Woon, 2011).

Thus, the findings provide fresh insights and a deeper understanding of how privacy awareness, security concerns and trust influence university students to share their personal information on social media platforms. Besides, it also reveals the three key elements that influence or hinder disclosure, allowing the pertinent parties to put in place the proper security measures to preserve their clients' privacy, lessen their perception of risk, and encourage disclosure (Kolotylo-Kulkarni et al., 2021).

This research is limited by the sample used that is focused on only university students, in a limited area of Selangor, which generalization of the findings should be made with caution. To increase the explanatory power of the framework, future studies may replicate this study but need to broaden the sample to include actual consumers.

REFERENCES

Aljohani M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users' privacy setting & information disclosure. *The Proceeding of 14th Australian Information Security Management Conference* 67-75. https://doi.org/10.4225/75/58a693deee893

Almadhoun, N., Dominic, P., & Woon, F. (2011). Perceived Security, Privacy, and Trust concerns within Social Networking Sites. *IEEE International Conference on Control System, Computing and Engineering*. 426-431. https://doi.org/10.1109/iccsce.2011.6190564

Ampong, G., Mensah, A., Adu, A., Addae, J., Omoregie, O. K. & Ofori, K. S. (2018). Examining self-disclosure on social networking sites: A flow theory and privacy perspective. *Behavioral Sciences. 8(6),* 1-17. https://doi.org/10.3390/bs8060058

Bagozzi, R. P. & Yi, Y. 2012. Specification, Evaluation, and Interpretation of Structural Equation Models. *Journal of the Academy of Marketing Science* 40(1): 8-34. https://doi.org/10.1007/s11747-011-0278-x

Baruh, L., Secinti, E., Cemalcilar, Z. (2017). Online privacy concerns and privacy management: a meta-analytical review. *J. Commun. 67*, 26–53. https://doi.org/10.1111/jcom.12276

Beldad, A. D. (2015). Sharing to be sociable, posting to be popular: factors influencing non-static personal information disclosure on Facebook among young Dutch users. *International Journal of Web Based Communities*, *11*(3/4), 357. https://doi.org/10.1504/ijwbc.2015.072132

Bernama. Malaysia ranks top 5 globally in mobile social penetration, highest in region. Retrieved January 31, 2019, from https://www.nst.com.my/lifestyle/bots/2019/01/456119/malaysia-ranks-top-5-globally-mobile-social-media-penetration-highest

Jai, T. M., & King, N. J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services*, *28*, 296–303. https://doi.org/10.1016/j.jretconser.2015.01.005

Bhattacherjee, A. 2012. *Social Science Research: Principles, Methods, and Practices*. 2nd edition. Zurich, Switzerland: Creative Commons Attribution

Cater, T. & Cater, B. 2010. Product and Relationship Quality Influence on Customer Commitment and Loyalty in B2b Manufacturing Relationships. *Industrial Marketing Management* 39(8): 1321-1333. https://doi.org/10.1016/j.indmarman.2010.02.006

Chiu, C.-M. & Wang, E. T. G. 2008. Understanding Web-Based Learning Continuance Intention: The Role of Subjective Task Value. *Information & Management* 45(3): 194-201. https://doi.org/10.1016/j.im.2008.02.003

Cho, H., Lee, J., Chung, S. (2010). Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. *Comput. Hum. Behav. 26 (5)*, 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3), 395–416. http://dx.doi.org/10.1177/1461444808101618

Clement, J (2020). *Social media-Statistics & Facts*. Retrieved from: https://www.statista.com/topics/1164/social-networks/

Dhami, A., Agarwal, N., Chakraborty, T., Singh, B. P., & Minj, J. (2013). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. *Proceedings of the 2013 3rd IEEE International Advance Computing Conference*, IACC 2013. 2, 465-469. http://dx.doi.org/10.1109/IAdCC.2013.6514270

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Dwyer, C., Roxanne Hiltz, S., Passerini, K., & Roxanne, S. (2007) Trust and Privacy Concerns Within Social Networking Sites: A Comparison of Facebook and MySpace. *AIS eLibrary*. 12-31. http://aisel.aisnet.org/amcis2007/339

Fairbairn, W., & Kessler, A. (2015). Practical Advice for Selecting Sample Sizes. *Dced*, (May), 1–11. Available from: https://www.enterprise-development.org/wpcontent/uploads/Practical_advice_for_selecting_sample_sizes_May2015.pdf

Flavián, C. and Guinalíu, M. (2006) 'Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site', *Industrial Management and Data Systems*, Vol. 106, No. 5, pp.601–620. https://doi.org/10.1108/02635570610666403

Fogel, J., Nehmad, E. (2009). Internet social network communities: risk taking, trust, and privacy concerns. *Computers in Human Behavior 25*, 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Fornell, C. & Larcker, D. F. 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research* 18(1): 39-50. https://doi.org/10.2307/3151312

Gao, S., Mokhtarian, P. L. & Johnston, R. A. 2008. Nonnormality of Data in Structural Equation Models. *Transportation Research Record: Journal of the Transportation Research Board* 2082(1): 116-124. https://doi.org/10.3141/2082-14

Garson, G. D. 2012a. *Structural Equation Modeling*. Asheboro, NC USA: Statistical Associates Publishing

Garson, G. D. 2012b. *Testing Statistical Assumptions*. Asheboro, NC USA: Statistical Associates Publishing

Gaskin, J. 2012a. Common Method Bias. *Gaskination's Statistics*. http://youtube.com/Gaskination [20th December 2021]

Gaskin, J. 2012b. Confirmatory Factor Analysis. *Gaskination's StatWiki*. http://statwiki.kolobkreations.com [20th December 2021]

Gaskin, J. 2013. Data Screening. *Gaskination's StatWiki*. https://www.youtube.com/watch?v=1KuM5e0aFgU [December 20, 2021]

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. ACM SIGMIS Database: Database Adv. *Inf. Syst. 33*, 38–53. https://doi.org/10.1145/569905.569910

Gouldner, A.W., (1960). The norm of reciprocity: a preliminary statement, Am. Sociol. Rev. 25 (2) 161–178. https://doi.org/10.2307/2092623

Grazioli S. & Jarvenpaa, S.L. (2000). Perlis of Internet Fraud: An Empirical Investigation of Deception and Trust with Internet Consumers. *Systems and Humans, 30(4),* 395-410. https://doi.org/10.1109/3468.852434

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice. 17(1),* 43-53. https://doi.org/10.1057/dddmp.2015.32

Hair, J. F., Black, W. C., Babin, B. J. & Anderson, R. E. 2010. *Multivariate Data Analysis: A Global Perspective*. 7th edition. Upper Saddle River, New Jersey: Pearson Education Inc

Hair, J. F., Sarstedt, M., Ringle, C. M. & Mena, J. A. 2012. An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research. *Journal of the Academy of Marketing Science* 40(3): 414-433. https://doi.org/10.1007/s11747-011-0261-6

Hall, H., Widén, G., & Paterson, L. (2010). Not what you know, nor who you know, but who you know already: Examining online information sharing behaviours in a blogging environment through the lens of social exchange theory. *Libri. 60(2),* 117-128. https://doi.org/10.1515/libr.2010.011

Haris@Harib, A. R., Sarijan, S., & Hussin, N. (2017). Information Security Challenges: A Malaysian Context. *International Journal of Academic Research in Business and Social Sciences*, *7*(9). https://doi.org/10.6007/ijarbss/v7-i9/3335

Hertzog, M. A. 2008. Considerations in Determining Sample Size for Pilot Studies. *Research in Nursing & Health* 31(2): 180–191. https://doi.org/10.1002/nur.20247

Hoadley, C.M.; Xu, H.; Lee, J.J.; Rosson, M.B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electron. Commer. Res. Appl. 9*, 50–60. https://doi.org/10.1016/j.elerap.2009.05.001

Homans, G. (1961). Social Behavior. New York: Harcourt, Brace & World

Jarvenpaa, S., Leidner, D. (1998). Communication and trust in global virtual teams. *Journal of Computer-Mediated Communication 3 (4).* https://doi.org/10.1111/j.1083-6101.1998.tb00080.x

JithiKrishna P P, Suresh Kumar R and Sreejesh V K, (2015). Impact of trust, privacy and security in Facebook information. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *4*(6), 5–9. Retrieved from: https://ijettcs.org/pabstract_Share.php?pid=IJETTCS-2015-10-29-7

Joe, M. (2014). A Survey of Various Security Issues in Online Social Networks. *International Journal of Computer Networks and Applications. 1(1),* 11-14. Available from: https://www.academia.edu/10360339/A_Survey_of_Various_Security_Issues_in_Online_Social_Networks

Kayes, I., Kourtellis, N., Bonchi, F., & Iamnitchi, A. (2015). Privacy concerns vs. user behavior in community question answering. *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, ASONAM 2015. 681-688. https://doi.org/10.1145/2808797.2809422

Kisekka, V.; Bagchi-Sen, S.; Rao, H.R. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Comput. Hum. Behav. 29*, 2722–2729. https://doi.org/10.1016/j.chb.2013.07.023

Kline, R. B. 2011. *Principles and Practice of Structural Equation Modeling*. 3rd edition. New York: The Guilford Press

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. Journal of Business Research, 126, 221-238. https://doi.org/10.1016/j.jbusres.2020.12.006

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krejcie, R.V. & Morgan, D.W. (1970). Determining sample size for research activities. *Educational & Psychological Measurement*, 30, 607-610. https://doi.org/10.1177/001316447003000308

Malaysian Communications and Multimedia Commission. (2017). Section 3: Main Findings. *Internet Users Survey 2017*, 8–34. Retrieved from http://search.proquest.com/docview/1477205997?accountid=14744%5Cnhttp://fama.us.es/search*spi/i?SEARCH=18434711%5Cnhttp://pibserver.us.es/gtb/usuario_acceso.php?centro=$USEG&centro=%24USEG&d=1

Malhotra N.K. (2002). Marketing Research: An Applied Orientation (4th Eds). United State, MA: *Pearson Education, Inc*

Masele, J. J. (2022). Information Sharing in the Social Media Era. *University of Dar Es Salaam Library Journal*, *16*(2), 202–222. https://doi.org/10.4314/udslj.v16i2.14

McKnight, D.H.; Lankton, N.; Tripp, J. (2011). Social Networking Information Disclosure and Continuance Intention: A Disconnect. *In Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS*), Washington, DC, USA, 4–7, pp. 1–10. https://doi.org/10.1109/HICSS.2011.379

Ministry of Education, M. (2019). Educational Planning and Research Division Ministry Of Education Malaysia With Best Compliments. Available from: https://www.moe.gov.my/menumedia/media-cetak/penerbitan/quick-facts/2722-quick-facts-2019/file

Mohd Azul Mohamad Salleh, Ali Salman & Nurul Madiha Mohd Ilham (2015). Kesedaran Terhadap Isu Pengawasan Sewaktu Mengguna Aplikasi Media Sosial. *Journal of Social Science and Humanities*, 10(2), 217-229. Retrieved from http://ejournal.ukm.my/ebangi/article/view/11259/3646

O'Bien, D.; Torres, A. (2012). Social Networking and Online Privacy: Facebook Users' Perceptions. *Ir. J. Manag. 31*, 63–97. Available from: https://aran.library.nuigalway.ie/handle/10379/4059

Padyab, A., Päivärinta, T., Ståhlbröst, A., Bergvall. K & Birgitta (2019). Awareness of Indirect Information Disclosure on Social Network Sites. *SAGE Journals*. 1-14. https://doi.org/10.1177/2056305118824199

Pallant, J. 2007. *Spss Survival Manual: A Step-by-Step Guide to Data Analysis Using Spss for Windows.* 3rd Edition. New York: Open University Press

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., Hidayanto, & Achmad, N. (2019). Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, twitter, and Instagram. *2018 International Conference on Advanced Computer Science and Information Systems*, ICACSIS 2018. 271-276. https://doi.org/10.1109/ICACSIS.2018.8618220

Perrin, A. (2015). Social Media Usage: 2005-2015, (October), 2005–2015. Retrieved from: www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

Petronio, S. (2004). Boundary of Privacy: Dialectics of Disclosure; State University of New York Press: Albany, NY, USA

Petronio, S.; Hernandez, R. (2019). Communication Privacy Management Theory. https://doi.org/10.1093/acrefore/9780190228613.013.373

Podsakoff, P. M., Mackenzie, S. B. & Podsakoff, N. P. 2012. Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual Review of Psychology* 63(1): 539-569. https://doi.org/10.1146/annurev-psych-120710-100452

Podsakoff, P. M., Mackenzie, S. B., Lee, J.-Y. & Podsakoff, N. P. 2003. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of applied psychology* 88(5): 879- 903. https://doi.org/10.1037/0021-9010.88.5.879

Ramayah, T., Lee, J. W. C. & Mohamad, O. 2010. Green Product Purchase Intention: Some Insights from a Developing Country. *Resources, Conservation and Recycling* 54(12): 1419-1427. https://doi.org/10.1016/j.resconrec.2010.06.007

Reddy, K. & Reddy, E. S. (2019). Integrated approach to detect spam in social media networks using hybrid features. *International Journal of Electrical and Computer Engineering (IJECE). 9(1),* 562. https://doi.org/10.11591/ijece.v9i1.pp562-569

Reisinger, Y. & Mavondo, F. 2007. Structural Equation Modeling. *Journal of Travel & Tourism Marketing* 21(4): 41-71. https://doi.org/10.1300/J073v21n04_05

Saleh Zolait, A., Al-Anizi, R., Ababneh, S., BuAsalli, F. and Butaiba, N. (2014). User awareness of social media security: The public sector framework. *International Journal of Business Information Systems. 17(3),* 261-282. https://doi.org/10.1504/IJBIS.2014.064973

Saleh, Zakaria and Mashour, A. (2016). Evaluating Security Awareness Impact On Perceived Risk and Trust: The Case of Social Networks. *International Journal in IT and Engineering*, *4*(5), 99–110. Available from: https://www.researchgate.net/publication/303700743_EVALUATING_SECURITY_AWARENESS_IMPACT_ON_PERCEIVED_RISK_AND_TRUST_THE_CASE_OF_SOCIAL_NETWORKS

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research Methods for Business Students. 5th edition. Essex: Pearson Education Limited

Savolainen, R. (2017). Information sharing and knowledge sharing as communicative activities. *Information Research*, *22*(3), 767. Available from: https://eric.ed.gov/?id=EJ1156371

Schumacker, R. E. & Lomax, R. G. 2004. *A Beginner's Guide to Structural Equation Modeling*. Second edition. Lawrence Erlbaum Associates

Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers. 22(5),* 428-438. https://doi.org/10.1016/j.intcom.2010.05.001

Sriratanaviriyakul, N., Nkhoma, M., Felipe, A. L., Cao, T. K., Ha Tran, Q., Epworth, R., Shankaranarayanan, A, Quang, H. Le. (2017). ASEAN users' privacy concerns and security in using online social networks. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 84–99. https://doi.org/10.1504/IJESDF.2017.081787

Surma, J. (2016). Social exchange in online social networks. the reciprocity phenomenon on Facebook. *Computer Communications*, *73*, 342–346. https://doi.org/10.1016/j.comcom.2015.06.017

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior. 29(3),* 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Tuunainen V. K., Pitkanen, O. and Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking Sites — Case Facebook. 22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety. https://aisel.aisnet.org/bled2009/42

Vemprala, N., & Dietrich, G. (2019). A Social Network Analysis (SNA) Study On Data Breach Concerns Over Social Media. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, *6*, 7186–7193. https://doi.org/10.24251/hicss.2019.862

Willoughby, M. (2018). A review of the risks associated with children and young people's social media use and the implications for social work practice. *Journal of Social Work Practice. 0533(5)*, 1-14. https://doi.org/10.1080/02650533.2018.1460587

Yuen Meikeng, Lim May Lee, & Clarissa Say, (2018). Our teens are bullies. Retrieved 18 March, 2018, from https://www.thestar.com.my/news/nation/2018/03/18/behaving-badly-in-cyberspace-malaysian-teens-more-likely-to-be-cyberbullies-than-victims-says-study

Zaefarian, G., Henneberg, S. C. & Naudé, P. 2013. Assessing the Strategic Fit between Business Strategies and Business Relationships in Knowledge- Intensive Business Services. *Industrial Marketing Management* 42(2): 260- 272. https://doi.org/10.1016/j.indmarman.2012.08.008

Zhang, Z., & Gupta, B.B. (2016). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, 86, 914- 925. https://doi.org/10.1016/j.future.2016.10.007

Zhou, T., Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concerns. *Comput. Hum. Behav. 37*, 283–289. https://doi.org/10.1016/j.chb.2014.05.008

Zlatolas, L. N., Welzer, T., Heričko, M. & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior. 45*, 158-167. https://doi.org/10.1016/j.chb.2014.12.012