Jurnal Komunikasi: Malaysian Journal of Communication
https://ejournal.ukm.my/mjc
Volume 41(3) 2025: 522-541

Predictors of Self-Disclosure Activities in Social Networking Sites (SNS) among University Students in Malaysia

ADILA ISMAIL
HABEE BULLAH AFFANDY*
MOHAMMAD REZAL HAMZAH
Universiti Malaysia Perlis

ABSTRACT

The widespread use of the Internet, especially social media, has raised new privacy concerns due to extensive online interactions and the sharing of personal information on social networking sites (SNS). This study examines users' self-disclosure behaviour on social media using the APCO Model (Antecedents - Privacy Concerns - Outcomes), supported by the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM). The study expands the APCO model by adding new antecedents predicting self-disclosure activities and includes trust and risk as moderators between privacy concerns and self-disclosure. Using a quantitative approach, a survey was conducted with 998 students from five Malaysian public universities. Structural Equation Modelling (SEM) was applied to test hypotheses regarding variable relationships and the roles of mediators and moderators. The findings reveal that privacy concerns negatively impact self-disclosure, while social identity and familiarity with big data have a direct influence. Privacy concerns fully mediate the effects of privacy invasion experiences and perceived control over self-disclosure. Additionally, trust and perceived risk moderate the relationship between privacy concerns and self-disclosure, showing differences between high and low groups. This research contributes valuable insights to the field of online self-disclosure and invites further academic exploration.

Keywords: *Privacy concerns, self-disclosure, social media, APCO model, trust and risk.*

INTRODUCTION

Since the advent of the internet, privacy has remained a paramount concern, especially with the proliferation of big data and social networking sites (SNS). Recent reports indicate that 33.1% of global users and 35.6% of Malaysians express apprehension regarding the misuse of their online data (Kemp, 2024). Major corporations like Google and Meta (formerly Facebook) often share user data with affiliates, heightening risks of identity fraud and privacy breaches (Doerr et al., 2023). To maintain user engagement, SNS platforms encourage content sharing, inadvertently increasing the potential for third-party data misuse. This phenomenon has led to growing awareness across all user demographics, including children and older adults, about the importance of online privacy (Alagood et al., 2023; Goyeneche et al., 2023).

A critical behaviour in this context is self-disclosure—the intentional sharing of personal information—which facilitates relationship building and personal well-being (Hossain et al., 2023; Gonsalves et al., 2023). However, users often grapple with the *privacy paradox*, where they value privacy yet willingly disclose personal information for perceived benefits (Cloarec et al., 2024; Hirschprung, 2023). This behaviour is explained by the Privacy Calculus Model, suggesting users weigh risks against rewards when deciding to share information (Fu et al., 2023; Meier & Krämer, 2024; Trepte et al., 2020).

*Corresponding author: habee@unimap.edu.my
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2025-4103-28
Received: 16 May 2025 | Accepted: 16 July 2025 | Published: 30 September 2025

Recent studies have expanded on these concepts. Meier and Krämer (2024) found that privacy behaviours on social media are shaped by perceived benefits and risks. Specifically, benefit perceptions were shown to increase users' intentions to disclose personal information, both across individuals and within the same person over time. Similarly, a study by Duong et al. (2024) found that Vietnamese university students exhibit low privacy concern on TikTok, with peer influence and societal norms significantly shaping their privacy attitudes and behaviours.

The commercial use of SNS has amplified privacy challenges, as platforms collect vast data for profiling and targeted advertising (Ghermandi, 2023; Ong & Toh, 2023). This has led to increased scrutiny from regulatory bodies such as the Federal Trade Commission (FTC) that reported major social media companies lack adequate privacy protections, collecting extensive user data without sufficient oversight (FTC, 2023). Additionally, users' profile data and features like news feeds expose them to risks such as fraud, harassment, and cyberbullying (Al-Turif & Al-Sanad, 2023; Georgieva et al., 2024; United Nations, 2025).

In short, while SNS platforms offer numerous benefits, they also pose significant privacy risks. Users must navigate the delicate balance between sharing personal information for social and functional gains and protecting their privacy in an increasingly data-driven digital landscape.

RESEARCH BACKGROUND

Recent research on youth self-disclosure and privacy concerns on social networking sites (SNS) reveals an evolving and complex landscape shaped by both individual and societal factors. Early studies highlighted that younger users often prioritised social engagement over privacy, sometimes underestimating potential risks (Hoofnagle et al., 2010; Benamati et al., 2016). However, more recent findings suggest that while many young people continue to use real names and photos on social media, they increasingly avoid sharing sensitive information (Vespoli et al., 2024), though their understanding of advanced privacy threats like data mining and profiling remains limited. In another study conducted by Valckx (2023), it is found that privacy awareness significantly influences privacy concerns, perceived privacy risk, and perceived privacy control, and indirectly affects willingness to disclose information through privacy concerns.

The integration of personality frameworks such as the Big Five into privacy research has shown that perceived risks discourage, while perceived benefits encourage, disclosure, with *Agreeableness* emerging as the only personality trait directly linked to greater self-disclosure (Alwahaishi et al., 2024). Before, a similar study was conducted by Tang et al. (2022), and the findings show that privacy behaviours on social media are strongly influenced by perceived benefits, risks, and trust, with benefit perceptions and trust increasing self-disclosure and authorisation intentions, while privacy concerns reduce willingness to share information. Agreeableness enhances trust, while *Neuroticism* undermines it. Rational decision-makers tend to perceive higher privacy risks, and intuitive users particularly benefit from decision-making aids like the privacy score. Finally, prior negative experiences raise privacy concerns, further reducing users' willingness to disclose personal data.

The well-known *privacy paradox*, where users express privacy concerns yet continue to disclose personal data, has been revisited through the concept of IT identity, revealing that users who view SNS as central to their self-concept are more prone to self-disclosure despite risks (Mosafer & Sarabadani, 2024). Additionally, trust and perceived risk play significant moderating roles: higher trust reduces privacy concerns and increases disclosure, while higher

risk amplifies concerns and reduces sharing (Ismail et al., 2024; Ismail et al., 2021b). Together, these studies highlight the need for improved digital literacy to help young users navigate the complex interplay of personality, perceived risks, trust, and external regulations in their online self-disclosure behaviours. As such, the purpose of this study is to identify the predictors of self-disclosure activities among youth in Malaysia. Four (4) specific research objectives have been developed for this study, as follows:

1) To identify the relationship between the antecedents and privacy concerns in self-disclosure activities among youth.
2) To identify the direct relationship between the antecedents (social identity, self-efficacy, and perceived control) and self-disclosure activities among youth.
3) To identify the influence of privacy concerns as a mediator on self-disclosure activities among youth.
4) To identify the influence of moderators (trust and perceived risks) on the relationship of privacy concerns and self-disclosure activities among youth.

LITERATURE REVIEW

Self-Disclosure

Sidney Jourard first introduced the concept of self-disclosure, defining it as revealing one's inner thoughts and feelings to others, which became foundational in psychology and communication research (Jourard, 1964; Petronio & Sargent, 2020). Over time, scholars characterised self-disclosure as sharing personal information to build interpersonal relationships, influenced by factors like audience, depth, and amount of disclosure (Cozby, 1972; Derlega & Chaikin, 1977; Omarzu, 2000). Theories suggest it serves self-expression, social connection, and relationship-building (Altman & Taylor, 1973; Derlega & Grzelak, 1979), with benefits like self-acceptance and social bonding (Mancinelli, 2019; Krämer & Schäwel, 2020).

SNS has become central to daily life, with users engaging in activities such as posting status updates, interacting with communities, and sharing content (Howe, 2024; Kocak et al., 2020). SNS is used to establish and maintain relationships, often leading to increased personal information disclosure (Huber & Martinaitytė, 2022; Fan et al., 2021). Users disclose more information online than in face-to-face interactions, influenced by the perceived anonymity SNS provides (Xu & Zhang, 2025). Disclosure can range from personal information shared for relationship building to more sensitive content shared for communicational value, informational value, and instrumental value (Fan et al., 2021). Self-disclosure on SNS is reciprocal, with users expecting similar transparency in return (Pu et al., 2021; Yang et al., 2019). Perceived value in SNS, whether utilitarian (ease of use) or hedonic (entertainment), can influence users' willingness to share personal information (Akdim et al., 2022; Jo, 2022; Yum & Kim, 2024).

Privacy Concerns, Trust, and Perceived Risks

Privacy concerns arise when users worry about how their personal information is accessed and used on SNS (Neves et al., 2024). Trust in SNS platforms and perceived risks of disclosing personal information play significant roles in users' willingness to share data online. Privacy concerns negatively impact the likelihood of users revealing personal information, while trust can encourage disclosure (Ismail et al., 2024; Lee & Jhou, 2025; Van der Schyff & Flowerday, 2023). Understanding these factors is crucial in assessing online self-disclosure behaviours.

Familiarity with Big Data

Big data refers to large volumes of diverse data that require advanced technology for analysis and transformation (Oussous et al., 2018). Companies, particularly in business and social media, use big data to analyse user behaviours and trends for marketing and customer relationship management (Odionu et al., 2024). The rise of big data has heightened privacy concerns, as users are increasingly aware of how their personal information is collected and used (Quach et al., 2022). While big data offers benefits, it also raises significant privacy issues, especially when personal data is used for commercial purposes (Munir et al., 2015; Yadav et al., 2024). Users' understanding of big data impacts their privacy concerns, with more informed individuals often expressing less worry about privacy (Alashoor et al., 2017; Ismail et al., 2021a).

Privacy Invasion Experience

Experience refers to gaining knowledge or ability through actions, which can significantly impact a person's feelings and perceptions (Oxford Languages, 2024). A privacy invasion occurs when someone intrudes into another's personal life without consent, potentially leading to legal consequences (Trakic et al., 2023). In the online world, users' activities are often tracked, and personal data can be shared with other organisations without consent (Privacy Rights Clearinghouse, 2023). Research shows that privacy invasions increase concerns about the misuse of personal information, especially on social media platforms where individuals disclose much of their private data (Chen et al., 2023). Users who have faced privacy violations tend to be more sensitive to privacy risks in the future (Ho et al., 2023).

Social Identity

Social identity involves an individual's sense of belonging to social groups and is linked to self-esteem and personal relationships (Abrams, 2001). Social Identity Theory suggests that people seek to maintain a positive social identity to enhance self-esteem (Manzi et al., 2023). On SNS, users often share personal details to connect with others, build relationships, and gain social support. This self-disclosure on SNS can improve well-being, increase social capital, and foster self-esteem (Kasmani et al., 2022). Social identity influences privacy preferences and self-disclosure, with individuals adjusting their privacy behaviours based on their group affiliations and social interactions (Gruzd et al., 2018; Zhang & Fu, 2020).

Self-Efficacy

Self-efficacy, as defined by Bandura (1994), is an individual's belief in their ability to plan and execute actions to achieve specific goals. It is not related to one's actual abilities, but rather the confidence in using those abilities effectively. High self-efficacy boosts personal achievement and well-being (Bandura, 1994). Recent research highlights that self-efficacy focuses on what one can achieve using their abilities, rather than their raw skills (Basileo et al., 2024; Lopez-Garrido, 2025). Self-efficacy impacts task persistence and effort; when perceived self-efficacy is high, individuals exert greater effort and endure longer in achieving goals (Bandura, 1997). This concept is critical in the context of SNS, where users' belief in their ability to manage privacy and share information affects their behaviour. High self-efficacy in using SNS reduces privacy concerns and encourages information sharing, as seen in research by Princi and Krämer (2020).

Users with higher self-efficacy in privacy management are more likely to use privacy controls and feel less anxious about privacy risks (Bartol et al., 2023; Lee et al., 2017). However, studies have shown mixed results about whether self-efficacy consistently reduces privacy concerns (Menon, 2021).

Perceived Control

Perceived control refers to the belief that individuals can regulate their behaviour and the outcomes of their actions, such as managing their privacy on SNS (Tao et al., 2024). SNS platforms provide privacy settings that allow users to control who can view their personal information, which in turn can reduce privacy concerns (Lumare et al., 2024). The concept of perceived control is closely tied to privacy, as users who feel they can manage their information are more likely to share it. Research indicates that users with control over their personal data experience lower privacy risks and greater trust in the platform (Hunter & Taylor, 2020). Privacy control systems help build trust and promote information disclosure (Lumare et al., 2024). However, despite offering extensive privacy options, many users still fail to adequately protect their information, a phenomenon known as the privacy paradox (Ho et al., 2023). The complexity of privacy settings on SNS may overwhelm users, preventing them from fully protecting their information (Neves et al., 2024). In summary, perceived control enhances self-disclosure by reducing privacy concerns, but users' ability to navigate privacy settings effectively plays a crucial role in safeguarding personal information.

CONCEPTUAL FRAMEWORK

The conceptual framework of this study is designed by reference to the underpinning theory of this study, the APCO (Antecedents - Privacy Concerns - Outcomes) Model adapted by Alashoor et al. (2017) from the original APCO Macro Model by Smith et al. (2011). In the original model, the APCO Macro Model suggests that the construct of privacy concerns will likely mediate the relationships between a set of antecedents (Smith et al., 2011). Alashoor et al. (2017) mentioned that their research theoretical contribution is to focus on how awareness of the concept and practices of big data impacts privacy concerns. Along with the familiarity of big data, there are also other antecedents studied, namely *perceived control*, *perceived vulnerability*, and *self-efficacy*. The researcher also included the construct of *trust* as a moderator for privacy concerns and privacy disclosure outcomes, as Alashoor et al. (2017) suggested.

Additionally, the researcher also developed several other research constructs in reference to the Theory of Planned Behaviour (TPB) (Ajzen, 1991) and the Extension of Technology Acceptance Model (TAM) (Venkatesh & Davis, 2000). Four (4) constructs are adapted from TPB, which are *Privacy Invasion Experience* and *Perceived Control*, derived from the construct *attitude*, *Privacy Concerns* adapted from *perceived behavioural control*, and the fourth construct derived from Theory of Planned Behaviour (TPB) to be used in this study is *Self-Disclosure Activities* derived from the construct of *behaviour*. The researcher also adopted four (4) other constructs from TAM. The first one is *experience*, adapted as *Privacy Invasion Experience*. The second construct derived from TAM is *image*, adapted as Social Identity. Last but not least, the fourth and final construct derived from TAM to be used in this study is *usage behaviour*, adapted as *Self-Disclosure Activities*.

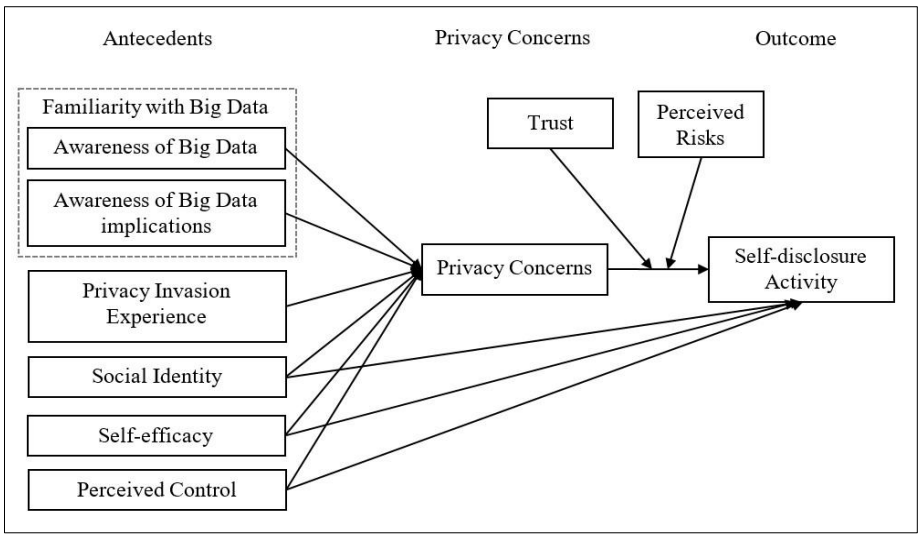


Figure 1: Conceptual framework

In this study, the familiarity of big data (awareness and awareness of big data implications), self-efficacy, and perceived control, as proposed by Alashoor et al. (2017), are retained as the independent variables, also referred to as antecedents. However, as highlighted in previous research, there are several other antecedents that may contribute to self-disclosure activities, such as privacy invasion experience and social identity. Therefore, these elements were also examined in this study to determine whether they influence self-disclosure activities on SNS. Along with trust, this study also included the construct of perceived risks as moderators in the relationship between privacy concerns and self-disclosure activities. These constructs are adapted from the original APCO macro model by Smith et al. (2011). Additionally, privacy concerns serve as the mediator variable, and finally, self-disclosure activities represent the dependent variable.

METHODOLOGY

A quantitative approach had been taken to complete this study through administrating a survey questionnaire. The population in the context of this study are youths who are pursuing their studies in public higher education. The decision to conduct this research at public universities was based on the stability of their student population. Unlike private universities, which often experience frequent changes in enrolment due to factors such as shorter program durations and higher student mobility, public universities offer a more consistent and reliable population for data collection.

In collecting the data, the researcher engaged with the undergraduate students (age range from 18-27). Survey questionnaires were distributed to students from five (5) random public universities in Malaysia. The universities are categorised into five (5) regions, namely Northern Region, East Coast Region, Central Region, Southern Region, and East Malaysia Region. Specifically, the basis of population determination is based on the statistics from the Department of Higher Education, Ministry of Education Malaysia where the statistics from the year 2023 is the year of reference for this study.

According to the statistics, the population frame for this research is 593,101. According to Krejcie and Morgan (1970), if the study population is greater than 100000, then the sample size is 384, taking into account that the degree of accuracy is 95%. The total responses collected is 998. The responses were recorded by using an online form formulated by using Google Forms.

DATA ANALYSIS

Structural Equation Model

In this study, the researcher used the AMOS software to come up with the structural equation model. To determine that the model fit used in this study is good, accurate, and good-fitting with the data, the researcher had used modification indices. The researcher had also used the item parcelling method. In conducting SEM analysis, the researcher had used two main steps; the first one is to predict the measurement model so that it can meet fit indices requirements. Next, the researcher then tested the model with the real data to answer the research hypotheses (Hair et al., 2010). This study is using absolute fit, incremental fit, and parsimonious fit indices to determine the model fit appropriate to the study data.

The analysis of the measurement model carried out includes Self-Disclosure Activities (3 items), Awareness of Big Data (4 items), Awareness of Big Data Implication (3 items), Privacy Invasion Experience (6 items), Social Identity (4 items), Self-Efficacy (4 items), Perceived Control (4 items), Privacy Concerns (5 items), Trust (5 items), and Perceived Risks (4 items). The results of the analysis indicate that all the model fit criteria have been met, with values for each indicator; GFI, CFI, IFI, TLI exceeding 0.90 and the RMSEA value shows less than 0.05 as stated by Hair (2010). The resulting match value is good for the measurement model which has been formed. The following is the model fit index; the value of $\chi 2$ = 1995.267, df = 771, p = 0.000, $\chi 2$/df = 2.588, GFI = 0.906, CFI = 0.952, NFI = 0.924, TLI = 0.946 and RMSEA = 0.040 (refer to Figure 2).

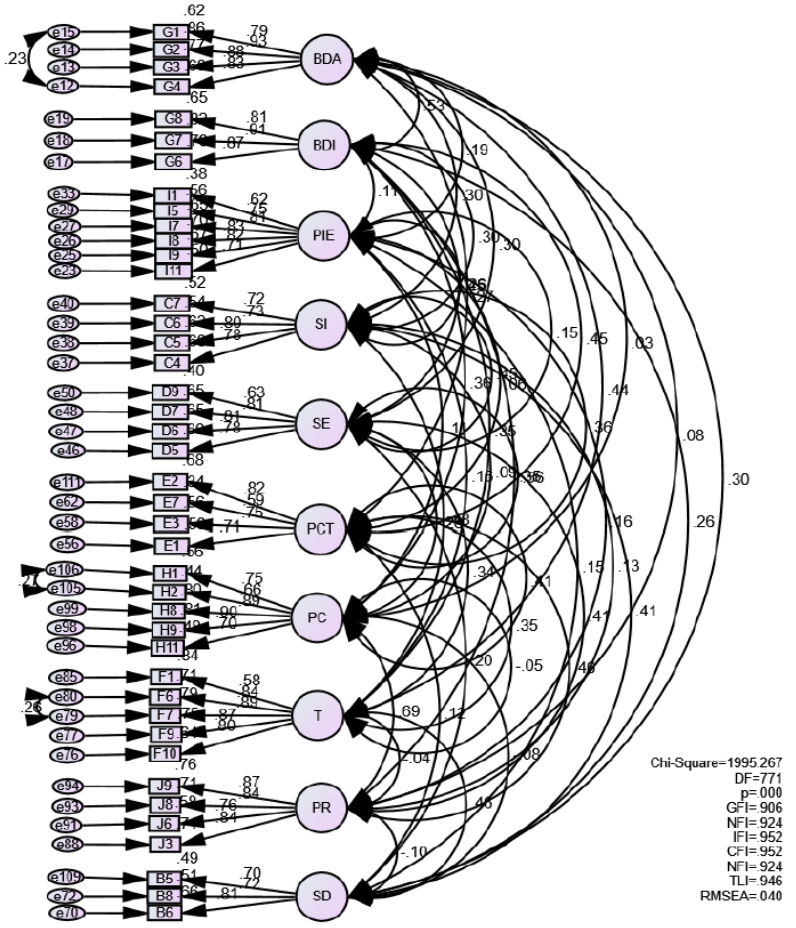


Figure 2: Structural equation model

Next, the validity of the constructs was done after the devising involvement with SEM to produce a better version of constructs for each variable. To that end, the researcher had used the Convergent Validity and Discriminant Validity Analysis (refer to Table 1). The condition of construct validation depends on the value of (1) Composite Reliability (CR), (2) Average Variance Extracted (AVE), (3) Maximum Shared Variance (MSV), and (4) Average Shared Variance (ASV). In this study, the researcher is following the suggestion of Hair et al. (2010) that a good construct must meet the following criteria: having a CR value that is greater than 0.7, having a good convergent validity value, which is AVE at 0.5, and having a value of discriminant validity, of which MSV is smaller than AVE value, and ASV is smaller than AVE value.

Table 1: Construct validation

Variable	**Reliability**	**Convergent validity**	**Discriminant validity**	
	CR >.07	AVE > 0.5	MSV < AVE	ASV < AVE
Self-Disclosure Activities	0.789	0.555	0.208	0.069
Big Data Awareness	0.916	0.733	0.280	0.095
Awareness of Big Data Implication	0.896	0.742	0.280	0.136
Privacy Invasion Experience	0.890	0.576	0.066	0.025
Social Identity	0.843	0.574	0.227	0.111
Self-Efficacy	0.843	0.575	0.319	0.137
Perceived Control	0.810	0.519	0.319	0.140
Privacy Concerns	0.888	0.617	0.480	0.099
Trust	0.900	0.647	0.227	0.113
Perceived Risks	0.900	0.692	0.480	0.116

Mediation Analysis

In this study, mediation analysis provides opportunities for researchers to determine if there are any variables involved as an intermediary if the results of multiple regressions are significant. This method is allowing researchers to identify the kinds of effects that exist in the relationship between variables, which are based on two categories: direct effects and indirect effects. Figure 3 shows the mediation analysis model for the study, which had been done using AMOS.

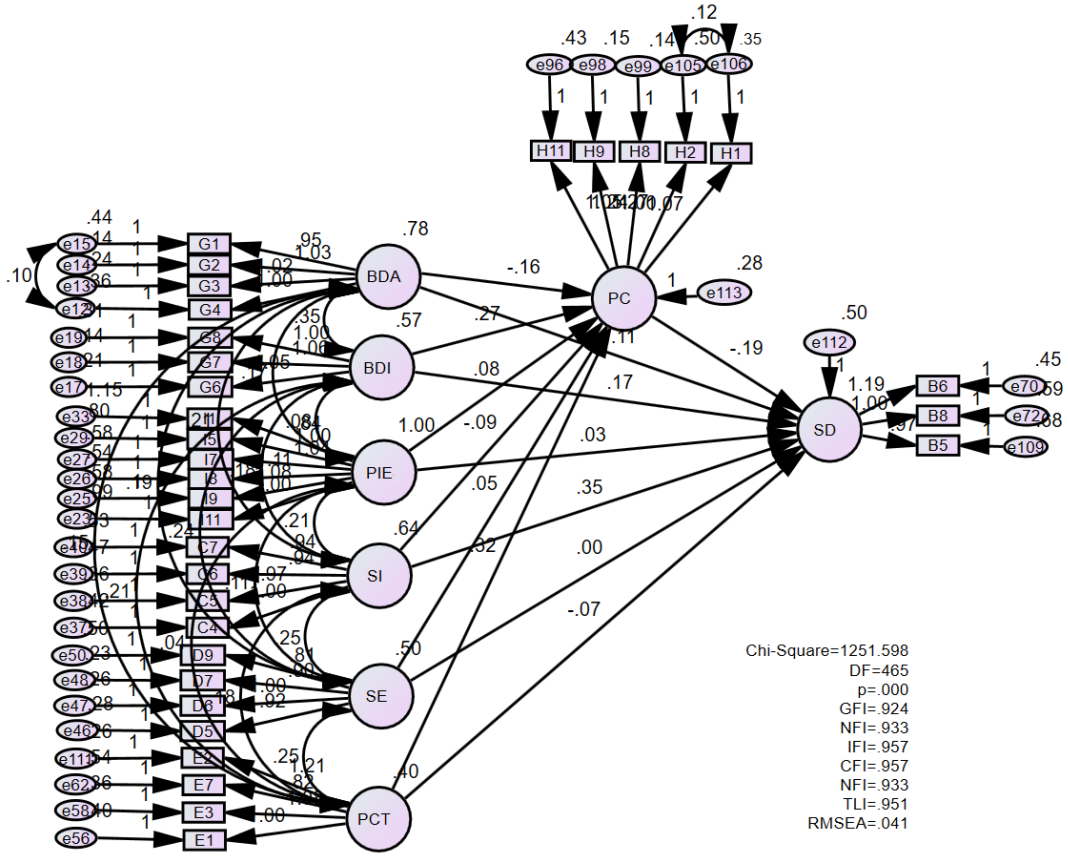


Figure 3: Full Mediation Model

Moderation Analysis

The key purpose of the moderation analysis is to measure and evaluate the different influences of the independent variable on the dependent variable as a moderator feature (Baron & Kenny, 1986). A basic moderation analysis, in particular, is necessary because the moderator is supposed to have an impact on the unique systemic path/paths supported by the underlying theory. A basic moderation effect can be measured by constructing a moderated regression model that describes whether the moderator changes the intensity and/or orientation of the interaction between the antecedent (independent variable) and the result (Andersson et al., 2014; Baron & Kenny, 1986). Customarily, a 'typical moderation model' is used, where the interaction effect between the independent variable and moderator variable needs to be computed in order to determine the significance level of a moderator (Awang, 2015).

However, in this study, the researcher had undertaken multigroup analysis (MGA) to analyse the moderation effects. This is due to the nature of the moderators in this study (trust and perceived risks), which are both categorical moderators, and the data are of an ordinal scale (Likert), which means a different group of higher/lower categories are expected to produce different outcomes. According to James Gaskin (2011), multigroup analysis in structural equation modelling (SEM) is another form of moderation analysis, but using categorical variables or grouping variables. It tests separate structural models in two or more groups. Such models may involve path models, comparison of indirect effects, confirmatory factor models, or full structural equation models (Jöreskog, 1971; Sorbom, 1974). Multigroup models generally follow the same structure in each group and can provide separate estimates

of within-group parameters (e.g., loadings, paths, and correlations). According to Chin and Dibbern (2010), the use of the z-test is adequate to put into practice multigroup analysis for a large sample size. In other words, the t-test for a large sample size is inadequate to be practiced since the elementary t-test is limited for a small sample size. The Z-test for two population proportions is used when the researcher wants to know whether two populations or groups are of significant difference on some influences of exogenous towards endogenous constructs.

The researcher followed the steps for conducting a multigroup analysis as recommended by Byrne (2016). In this study, multigroup analysis was done by first separating the higher and lower groups based on the moderators (trust and perceived risks respectively) by using median split in SPSS. Later on, each group model (High Trust and Low Trust, High Perceived Risks and Low Perceived Risks) was run in the AMOS software, where critical ratios (z-scores) are used to identify significant differences between groups on each path (Byrne, 2016), and compared to assess whether the slopes in the two groups (high and low) differ significantly. The path is considered different across groups when the P-value is significant (less than 0.50 or 0.10). If the absolute value of the z-score is greater than 1.96, then it is significant at the 0.05 level (James Gaskin, 2011). In this study, multigroup moderation analysis was conducted by using SPSS and AMOS. Excel Macros—Stats Tools Package by Gaskin (2016) was also utilised.

RESULTS AND DISCUSSION

Relationship Between the Antecedents and Privacy Concerns in Self-Disclosure Activities

Privacy concerns on social networking sites (SNS) are influenced by various factors, including familiarity with big data, privacy invasion experiences, social identity, self-efficacy, and perceived control. Privacy concerns negatively impact self-disclosure, as users are reluctant to share personal information due to fear of misuse. Awareness of big data technologies tends to decrease privacy concerns, as users accept the trade-off between privacy and technological benefits, though awareness of its implications—such as the risks of misuse for fraud or identity theft—can increase concerns. Users with past privacy invasion experiences exhibit stronger concerns, associating these experiences with future risks. Social identity plays a role in reducing privacy concerns, as individuals may prioritise self-image and social connections over privacy, particularly among younger users. Interestingly, self-efficacy, which refers to confidence in one's ability to manage SNS settings, does not significantly affect privacy concerns or self-disclosure in this study, contradicting previous research. Similarly, perceived control over privacy settings generally reduces privacy concerns, but this study found that users with more control might still feel uncertain about the security of their information, particularly when aware of how platforms exploit personal data. These findings highlight the complex, context-dependent nature of privacy concerns, self-disclosure, and the influence of individual antecedents.

Table 2: Correlation among antecedents, mediator (privacy concerns), and self-disclosure activities

Antecedent	Variable	*r*	*p*	Relationship Strength
Privacy concerns	Self-disclosure	-.147	***	Weak negative
Awareness of big data	Self-disclosure	.117	.008	Weak positive
Awareness of big data implications	Self-disclosure	.158	.001	Weak positive
Privacy invasion experience	Self-disclosure	.033	.364	Not significant
Social identity	Self-disclosure	.350	***	Moderate positive
Self-efficacy	Self-disclosure	.002	.968	Not significant

Perceived control	Self-disclosure	-.052	.312	Not significant
Awareness of big data	Privacy concerns	-.235	***	Weak negative
Awareness of big data implications	Privacy concerns	.333	***	Moderate positive
Privacy invasion experience	Privacy concerns	.124	***	Weak positive
Social identity	Privacy concerns	-.118	.003	Weak negative
Self-efficacy	Privacy concerns	.055	.224	Not significant
Perceived control	Privacy concerns	.327	***	Moderate positive

Note: Significance level (P Value ≤ 0.05)

Direct Relationship Between Antecedents and Self-Disclosure Activities

Despite privacy concerns, users are motivated to share personal information due to the desire to be part of the online community, leading to the privacy paradox—users claim concern for privacy but continue to disclose information. Social identity plays a significant role in promoting self-disclosure, as users seek to build relationships and receive social support. Awareness of big data's benefits also reduces privacy concerns, encouraging self-disclosure. Interestingly, awareness of big data's implications heightens privacy concerns but does not prevent self-disclosure, demonstrating the privacy paradox.

Privacy Concerns as a Mediator in Self-Disclosure Activities Among Youth

Privacy concerns play a mediating role in the relationship between antecedents and self-disclosure. The study finds that privacy concerns decrease self-disclosure, and in some cases, they fully mediate the relationship between antecedents (e.g., privacy invasion experience) and self-disclosure activities. Although privacy concerns can discourage self-disclosure, other motivations like social recognition and social contact may override these concerns, leading users to share personal information. The findings suggest that self-disclosure decisions are influenced by a balance of costs and benefits, with users selectively sharing certain types of information while protecting more sensitive data.

Table 3: Predictors of privacy concerns and self-disclosure activities

Variable	Model 1		Model 2		Model 3		Model 4	
	Beta (β)	*Sig. (ρ)*	*Beta (β)*	*Sig. (ρ)*	*Beta (β)*	*Sig. (ρ)*	*Beta (β)*	*Sig. (ρ)*
Awareness of big data	**-.165**	***	**.139**	***	**-.165**	***	**.107**	**.008**
Awareness of big data implications	**.272**	***	**.115**	**.022**	**.272**	***	**.169**	**.001**
Privacy invasion experience	**.076**	***	.012	.680	**.076**	***	.027	.364
Social identity	**-.091**	**.003**	**.370**	***	**-.091**	**.003**	**.353**	***
Self-efficacy	.048	.224	-.009	.879	.048	.224	.002	.968
Perceived control	**.319**	***	**-.125**	**.049**	**.320**	***	-.066	.312
Privacy concerns (mediator)	-	-	-	-	-	-	**-1.92**	***
R Square	**0.264**		**0.264**		**0.211**		**0.228**	

Note: Self-disclosure activities is the dependent variable
Model 1= Antecedents and mediator
Model 2= Antecedents and dependent variable
Model 3= Self-disclosure activities in the whole model
Model 4= Self-disclosure activities with mediator included in the model

Influence of Moderators (Trust and Perceived Risks) on Privacy Concerns and Self-Disclosure Activities

Trust and perceived risks serve as moderators in the relationship between privacy concerns and self-disclosure. Trust positively influences self-disclosure, as users are more likely to share personal information when they trust the SNS platform. Conversely, higher perceived risks negatively affect self-disclosure, as users are cautious about sharing personal information due to concerns over data misuse. The study shows that increased trust encourages self-disclosure, while higher perceived risks discourage it, supporting previous research that highlights the importance of trust and risk perception in online behaviour.

Table 4: Multigroup analysis based on trust in between the relationship of privacy concerns with self-disclosure activities

Path	**Low Level of Trust**		**High Level of Trust**		***Z*-Score (group difference)**
	Estimate	*ρ*	Estimate	*ρ*	
Privacy concerns → Self-disclosure activities	-0.140	0.003	0.101	0.204	2.612***

Table 5: Multigroup analysis based on perceived risks in between the relationship of privacy concerns with self-disclosure activities

Path	**Low Level of Perceived Risks**		**High Level of Perceived Risks**		***Z*-Score (group difference)**
	Estimate	*ρ*	Estimate	*ρ*	
Privacy concerns → Self-disclosure activities	0.176	0.026	-0.199	0.078	-2.722***

Novelty of the Study

Overall, there are a number of predictors that have been found as strong determinants of self-disclosure activities among youth in Malaysia. This study has proven that APCO Model is suitable in the context of this study, with the inclusion of privacy paradox phenomena. Figure 4 shows the modified conceptual framework, taking into accounts the results of the whole study. One variable, self-efficacy is removed from the original framework, as the results of the analyses show that there is not one relationship found between the proposed variable with the mediator or the outcome. All of the other variables are maintained and improved, which are awareness of big data, awareness of big data implication, privacy invasion experience, social identity as an independent variable/antecedent, privacy concerns as the mediator, and self-disclosure activities as the outcome.

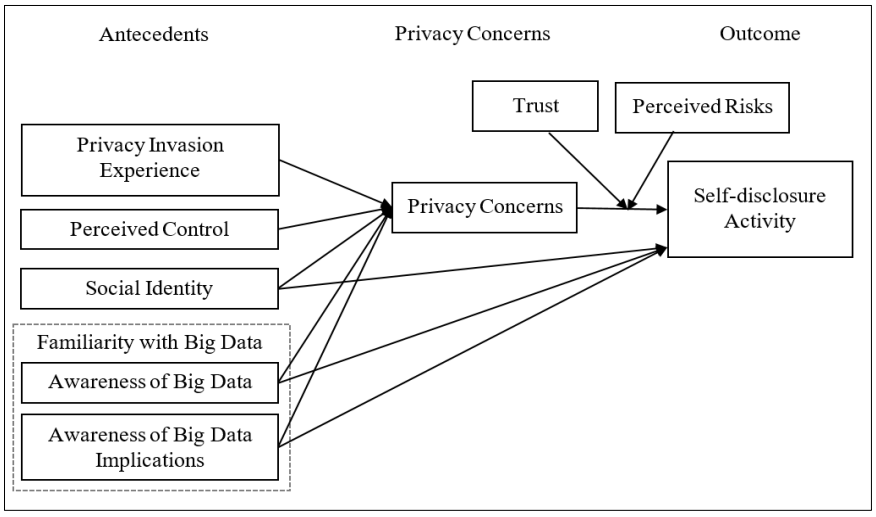


Figure 4: Modified model

Therefore, this research also gives a good basis for future researchers to test on various other features of SNSs apart from those proposed in the research model, such as sharing of photos/videos/locations or other specific types of information or formats, and also in the circumstance of specific SNSs such as YouTube, Facebook, Twitter, TikTok, and the like. This research is expected to foster interest and future study of the diverse dimensions of online self-disclosure.

CONCLUSION

Future studies should consider expanding the sample population to include diverse age groups, such as early-aged and middle-aged youths. By exploring a broader age range, researchers can examine how self-disclosure behaviours differ among various cohorts. Additionally, self-disclosure is not exclusive to younger users, so it is crucial to include older individuals who did not grow up with the internet. Another important consideration is the study of cultural variations, as self-disclosure is influenced by individual, cultural, and environmental factors. While this study was restricted to Malaysia, it is necessary to examine how different cultures may impact users' self-disclosure behaviours.

Furthermore, researchers should explore comparative studies by replicating this research on other social media platforms, such as messaging apps or dating sites, to understand the self-disclosure behaviour across various platforms. Future studies should also consider different research designs, such as qualitative methods like content analysis or experimental research with pre- and post-results. Additionally, future researchers should explore areas related to, but not limited to, the context of this study. Longitudinal research could offer deeper insights into the evolution of self-disclosure behaviours over time.

Another recommendation is the adoption of other developed models and theories in the context of self-disclosure or social media behaviours. The current study's findings show that only 22.8% of the self-disclosure activities in social networking sites (SNS) can be explained by the predictors in the model. This suggests that additional variables and processes need to be included in future studies to provide a more comprehensive understanding of self-disclosure in SNS.

CONCLUSION

Social media platforms have transformed the way individuals communicate, leaving behind significant digital footprints. Users share personal information like names, email addresses, locations, and interests when registering for social media accounts. In addition, user activity is tracked, such as when, where, and with whom they interact. This information is often shared with third-party organisations, sometimes without user consent, and is primarily used for targeted marketing.

Despite growing concerns about privacy, users' behaviours on SNS often contradict these concerns, resulting in a paradox of privacy. This paradox contributes to rising issues such as account hacking, impersonation, harassment, and stalking. These privacy violations are likely to increase, yet simply disconnecting from social media is not the solution. Users must understand the importance of avoiding oversharing personal information on SNS to mitigate these risks. The privacy concerns are genuine, and failure to secure personal data could lead to significant consequences.

This study expands on previous research by identifying predictors of self-disclosure activities, including privacy concerns as a mediator, and trust and perceived risk as moderating variables. Through an online survey conducted with students from Malaysian public universities, the study explored factors contributing to self-disclosure and their relationships. The findings revealed that privacy concerns negatively impact self-disclosure, while trust, social identity, and awareness of big data are key to fostering self-disclosure activities.

However, there are limitations to this study, including the self-reported nature of the survey, a limited timeframe for data collection, and a narrow age range. These limitations should be addressed in future studies, which could also explore other social media platforms such as messaging apps (e.g., WhatsApp, Telegram) or dating sites, as they are closely tied to privacy concerns and self-disclosure behaviours. Additionally, this study highlights the need for clearer privacy regulations in Malaysia, as well as greater public education about data collection, misuse, and legal protections against privacy violations.

The study also underscores the importance of big data awareness, as it has a growing impact on how individuals interact with businesses and institutions. Understanding how big data affects privacy and disclosure behaviours is crucial for developing new privacy theories. This research contributes to the academic literature by exploring the various antecedents, privacy concerns, trust, and perceived risks involved in self-disclosure, and it aims to inspire further interest and research in this area.

BIODATA

Dr. Adila Ismail is a senior lecturer at Universiti Malaysia Perlis (UniMAP) with expertise in new media technology, social media privacy, interpersonal communication, and information technology. Her research interests focus on the dynamics of digital interaction, particularly in the areas of privacy, self-disclosure, and communication behavior on social media platforms. Email: adilaismail@unimap.edu.my

Dr. Habee Bullah Affandy is a senior lecturer at Universiti Malaysia Perlis (UniMAP). His academic and research interests include web design, web usability, aesthetic design, information technology, and human-computer interaction. Dr. Habee is passionate about exploring how user-centered design principles can improve digital interfaces and enhance the overall user experience. Email: habee@unimap.edu.my

Assoc. Prof. Dr. Mohammad Rezal Hamzah is a senior lecturer at Universiti Malaysia Perlis (UniMAP) with expertise in communication, health communication, media and health, as well as youth and health studies. His research interests lie at the intersection of media, health awareness, and youth engagement, focusing on how communication strategies can influence public health outcomes. Email: rezal@unimap.edu.my

REFERENCES

Abrams, D. (2001). Social identity, psychology of. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia Of The Social & Behavioral Sciences* (pp. 14306–14309). Pergamon. https://doi.org/10.1016/B0-08-043076-7/01728-9

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Akdim, K., Casaló, L. V., & Flavián, C. (2022). The role of utilitarian and hedonic aspects in the continuance intention to use social mobile apps. *Journal of Retailing and Consumer Services, 66,* 102888. https://doi.org/10.1016/j.jretconser.2021.102888

Alagood, J., Prybutok, G., & Prybutok, V. R. (2023). Navigating privacy and data safety: The implications of increased online activity among older adults post-COVID-19 induced isolation. *Information, 14*(6), 346. https://doi.org/10.3390/info14060346

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems, 41,* 62–96.

Altman, I., & Taylor, D. A. (1973). *Social Penetration: The Development of Interpersonal Relationships.* Holt, Rinehart & Winston.

Al-Turif, G. A. R., & Al-Sanad, H. A. R. (2023). The repercussions of digital bullying on social media users. *Frontiers in Psychology, 14*, 1280757. https://doi.org/p7f8

Alwahaishi, S., Al-Ahmadi, M. S., Ali, Z., & Al-Jabri, I. (2024). Self-disclosure on social media: Do personality traits matter? *SAGE Open, 14*(2). https://doi.org/p7f9

Andersson, U., Cuervo-Cazurra, A., & Nielsen, B. B. (2014). From the editors: Explaining interaction effects within and across levels of analysis. *Journal of International Business Studies, 45*(9), 1063–1071. https://doi.org/10.1057/jibs.2014.50

Awang, Z. (2015). *SEM Made Simple: A Gentle Approach to Learning Structural Equation Modelling.* MPWS Rich Publication.

Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran (Ed.), Encyclopedia of Human Behavior (Vol. 4, pp. 71–81). Academic Press.

Bandura, A. (1997). Self-efficacy: The exercise of control. W.H. Freeman.

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51,* 1173–1182. https://doi.org/d7bst5

Bartol, J., Vehovar, V., Bosnjak, M., & Petrovčič, A. (2023). Privacy concerns and self-efficacy in e-commerce: Testing an extended APCO model in a prototypical EU country. *Electronic Commerce Research and Applications, 60*, 101289. https://doi.org/p7gb

Basileo, L. D., Otto, B., Lyons, M., Vannini, N., & Toth, M. D. (2024). The role of self-efficacy, motivation, and perceived support of students' basic psychological needs in academic achievement. *Frontiers in Education, 9*, 1385442. https://doi.org/p7gc

Benamati, J., Serva, M. A., & Fuller, M. A. (2016). Are trust and distrust distinct constructs? An empirical study of the effects of trust and distrust among online banking users. *Information Systems Management, 33*(1), 2–20.

Byrne, B. M. (2016). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming* (3rd Ed.). Routledge. https://doi.org/p7gd

Chen, S., Gu, C., Wei, J., & Lv, M. (2023). Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator. *Frontiers in Psychology, 13*, 1031592. https://doi.org/10.3389/fpsyg.2022.1031592

Chin, W. W., & Dibbern, J. (2010). An introduction to a permutation based procedure for Multi-Group PLS Analysis: Results of tests of differences on simulated data and a cross cultural analysis of the sourcing of information system services between Germany and the USA. In V. E. Vinzi, W. W. Chin, J. Henseler & H. Wang (Eds.), *Handbook of Partial Least Squares: Concepts, Methods and Applications* (pp. 171–193). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-32827-8_8

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media. *Journal of Marketing Management, 41*(7), 1574–1596. https://doi.org/10.1002/mar.21998

Cozby, P. C. (1972). Self-disclosure, reciprocity and liking. *Sociometry, 35,* 151–160. https://doi.org/10.2307/2786555

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102–115. https://doi.org/10.1111/j.1540-4560.1977.tb01885.x

Derlega, V. J., & Grzelak, J. (1979). Appropriateness of self-disclosure. In G. J. Chelune & Associates (Eds.), *Self-disclosure: Origins, Patterns, and Implications of Openness in Interpersonal Relationship*. Jossey-Bass.

Doerr, S., Frost, J., Gambacorta, L., & Shreeti, V. (2023, October 16). *Big Techs in Finance* (BIS Working Papers No. 1129). Bank for International Settlements. https://www.bis.org/publ/work1129.htm

Duong, H. L., Tran, M. T., Vo, T. K. O., & Tran, T. K. C. (2024). Social media and privacy concerns: Exploring university student's privacy concerns in TikTok platform in Vietnam. *Journal of Information, Communication and Ethics in Society, 22*(4), 392–418. https://doi.org/10.1108/JICES-04-2024-0045

Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2021). Research on influencing factors of personal information disclosure intention of social media in China. *Data and Information Management, 5*(1), 195–207. https://doi.org/10.2478/dim-2020-0038

Federal Trade Commission (FTC). (2024). The Federal Trade Commission 2023 Privacy and Data Security Update. https://www.ftc.gov/reports/federal-trade-commission-2023-privacy-data-security-update

Fu, J., Zhang, J., & Li, X. (2023). How do risks and benefits affect users' privacy decisions? An event-related potential study on privacy calculus process. *Frontiers in Psychology, 14,* 1052782. https://doi.org/10.3389/fpsyg.2023.1052782

Gaskin, J. (2016). Stats Tools Package. *Gaskination's StatWiki.*

Georgieva, M., Sabeva, P., Mahmud, S., Sabeva, V., Tsanova, M., Kitanovski, V., Hauser, P., & Marzec-Balinow, K. (2024). Research on Current Risks Among Young People as Users of Social Networks. *Zenodo.* http://dx.doi.org/10.5281/zenodo.14844352

Ghermandi, A., Langemeyer, J., Van Berkel, D., Calcagni, F., Depietri, Y., Egarter Vigl, L., Fox, N., Havinga, I., Jäger, H., Kaiser, N., Karasov, O., McPhearson, T., Podschun, S., Ruiz-Frau, A., Sinclair, M., Venohr, M., & Wood, S. A. (2023). Social media data for environmental sustainability: A critical review of opportunities, threats, and ethical use. *One Earth, 6*(3), 236–250. https://doi.org/10.1016/j.oneear.2023.02.008

Gonsalves, P. P., Nair, R., Roy, M., Pal, S., & Michelson, D. (2023). A systematic review and lived experience synthesis of self-disclosure as an active ingredient in interventions for adolescents and young adults with anxiety and depression. *Administration and Policy in Mental Health, 50*(3), 488–505. https://doi.org/10.1007/s10488-023-01253-2

Goyeneche, D., Singaraju, S., & Arango, L. (2023). Linked by age: A study on social media privacy concerns among younger and older adults. *Industrial Management & Data Systems, 124*(6), 2401-2418. https://doi.org/10.1108/IMDS-07-2023-0462

Gruzd, A., & Hernández-García, Á. (2018). Privacy concerns and self-disclosure in private and public uses of social media. *Cyberpsychology, Behavior, and Social Networking, 21*(7), 418–428. https://doi.org/10.1089/cyber.2017.0709

Hair, J. F., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis: A global perspective* (7th ed.). Prentice Hall.

Hirschprung, R. S. (2023). Is the privacy paradox a domain-specific phenomenon. *Computers, 12*(8), 156. https://doi.org/10.3390/computers12080156

Ho, F. N., Ho-Dac, N., & Huang, J. S. (2023). The effects of privacy and data breaches on consumers' online self-disclosure, protection behavior, and message valence. *SAGE Open, 13*(3). https://doi.org/10.1177/21582440231181395

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.1589864

Hossain, Md. M., Islam, K. M. Z., Al Masud, A., Hossain, Md. A., & Jahan, N. (2023). Antecedents and consequences of self-disclosure in subjective well-being: A Facebook case with a social support mediator. *SAGE Open, 13*(2). https://doi.org/p7gg

Howe, S. (2024). *Social media statistics for Malaysia* [Updated 2024]. We are Social; Meltwater. https://www.meltwater.com/en/blog/social-media-statistics-malaysia

Huber, L., & Martinaitytė, M. (2022). Relationships in the digital age: Self-disclosure and Communication in Social Networking Sites. *European Integration Studies, 1*(16), 24–40. https://doi.org/10.5755/j01.eis.1.16.31632

Hunter, G. L., & Taylor, S. A. (2020). The relationship between preference for privacy and social media usage. *Journal of Consumer Marketing, 37*(1), 43–54. https://doi.org/gpbtw8

Ismail, A., Hamzah, M. R., & Hussin, H. (2021a). Conceptual paper: Sentience of big data towards user privacy concerns and online self-disclosure activities. *Emerging Advances in Integrated Technology, 2*(2), 38–42.

Ismail, A., Hamzah, M. R., & Hussin, H. (2021b). The roles of trust and perceived risks on online self-disclosure. *AIP Conference Proceedings, 2347*, 020191. https://doi.org/p7gj

Ismail, A., Hamzah, M. R., & Hussin, H. (2024). Self-disclosure on SNS: Trust and perceived risks as moderators. *AIP Conference Proceedings, 2799*, 020084. https://doi.org/p7gk

James Gaskin. (2011, Aug 26). *Multigroup moderation in Amos - Made easy (with critical ratios)* [Video]. YouTube. https://www.youtube.com/watch?v=ZMYS90AU8bs

Jo, H. (2022). Antecedents of continuance intention of social networking services (SNS): Utilitarian, hedonic, and social contexts. *Mobile Information Systems*, *2022*(1), 7904124. https://doi.org/10.1155/2022/7904124

Jöreskog, K. G. (1971). Simultaneous factor analysis in several populations. *Psychometrika, 36*(4), 409–426. https://doi.org/10.1007/BF02291366

Jourard, S. M. (1964). *The Transparent Self*. Van Nostrand Reinhold Inc.

Kasmani, F., Abdul Aziz, A. R., & Sawai, R. (2022). Self-disclosure on social media and its influence on the well-being of youth. *Jurnal Komunikasi: Malaysian Journal of Communication, 38*(3), 272–290. https://doi.org/10.17576/JKMJC-2022-3803-17

Kemp, S. (2024). *Digital 2024: Global Overview Report.* DataReportal; We Are Social & Meltwater. https://datareportal.com/reports/digital-2024-global-overview-report

Kocak, E., Nasir, V. A., & Turker, H. B. (2020). What drives Instagram usage? User motives and personality traits. *Online Information Review, 44*(3), 625-643. https://doi.org/grr2dt

Krämer, N. C., & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology, 31*, 67–71.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and Psychological Measurement, 30(3), 607–610. https://doi.org/ggb4r2

Lee, C. W., & Jhou, Y. T. (2025). Understanding self-disclosure in social networking sites: The influence of trust and perceived privacy risk. *Journal of Applied Finance & Banking, 15*(1), 111–131. https://doi.org/10.47260/jafb/1516

Lee, W., Tan, C.-S., & Siah, P. C. (2017). The role of online privacy concern as a mediator between internet self-efficacy and online technical protection privacy behavior. *Sains Humanika, 9*(3-2), 1–10. https://doi.org/10.11113/sh.v9n3-2.1271

Lopez-Garrido, G. (2025). Bandura's self-efficacy theory of motivation in psychology. *Simply Psychology*. https://www.simplypsychology.org/self-efficacy.html

Lumare, N., Muradyan, L., & Jansberg, C. (2024). Behind the screen: The relationship between privacy concerns and social media usage. *Journal of Marketing Communications, 30*(4), 417–432. https://doi.org/10.1080/13527266.2024.2424922

Mancinelli, J. M. (2019). The effects of self-disclosure on the communicative interaction between a person who stutters and a normally fluent speaker. *Journal of Fluency Disorders, 59*, 1–20. https://doi.org/10.1016/j.jfludis.2018.11.003

Manzi, C., Paderi, F., & Benet-Martinez, V. (2023, December 8). Multiple social identities and well-being: Insights from a person-centred approach. *British Journal of Social Psychology, 63*(2), 792-810. https://doi.org/10.1111/bjso.12704

Meier, Y., & Krämer, N. C. (2024). The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels. *Communication Research, 51*(2), 178-202. https://doi.org/10.1177/00936502221102101

Menon, M. (2021, Nov 30). Self-efficacy and privacy concerns predict reported use of privacy controls on Messenger. *TTC Labs.* https://www.ttclabs.net/research/self-efficacy-and-privacy-concerns-predict-reported-use-of-privacy-controls

Mosafer, H., & Sarabadani, J. (2024). Exploring the privacy paradox: The role of IT identity in self-disclosure on social networking sites. *European Conference on Information Systems (ECIS) 2024 Proceedings, 16.*

Munir, A. B., Yasin, S. H. M., & Muhammad-Sukki, F. (2015). Big data: Big challenges to privacy and data protection. *International Scholarly and Scientific Research & Innovation, 9*(1).

Neves, J., Turel, O., & Oliveira, T. (2024). Privacy concerns in social media use: A fear appeal intervention. *International Journal of Information Management Data Insights, 4*(2), 100260. https://doi.org/10.1016/j.jjimei.2024.100260

Odionu, C. S., Bristol-Alagbariya, B., & Okon, R. (2024). Big data analytics for customer relationship management: Enhancing engagement and retention strategies. *International Journal of Scholarly Research in Science and Technology, 5*(2), 050–067. https://doi.org/10.56781/ijsrst.2024.5.2.0039

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review, 4*(2), 174–185. https://doi.org/10.1207/S15327957PSPR0402_05

Ong, B., & Toh, D. J. (2023). Digital dominance and social media platforms: Are competition authorities up to the task? *IIC - International Review of Intellectual Property and Competition Law, 54*(4), 527–572. https://doi.org/10.1007/s40319-023-01302-1

Oussous, A., Benjelloun, F.-Z., Ait Lahcen, A., & Belfkih, S. (2018). Big data technologies: A survey. *Journal of King Saud University - Computer and Information Sciences, 30*(4), 431–448. https://doi.org/10.1016/j.jksuci.2017.06.001

Oxford Languages. (2024). *Definition of Experience*. Oxford University Press.

Petronio, S., & Sargent, J. (2020). Self-disclosure: Gender differences, family privacy, parents and child privacy. The Marriage and Family Encyclopedia. *JRank.* https://family.jrank.org/pages/1474/Self-Disclosure.html

Princi, E., & Krämer, N. (2020). Out of control - Privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology, 11*, 582054. https://doi.org/10.3389/fpsyg.2020.582054

Privacy Rights Clearinghouse. (2023). Privacy basics: Understanding data collection online.

Pu, W., Li, S., Bott, G., Esposito, M., & Thatcher, J. (2021). To disclose or not to disclose: An evaluation of the effects of information control and social network transparency. *Computers & Security, 112,* 102509. https://doi.org/10.1016/j.cose.2021.102509

Quach, S., Thaichon, P., Martin, K.D. et al. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science, 50,* 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Smith, J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015. https://doi.org/10.2307/41409970

Sorbom, D. (1974). A general method for studying differences in factor means and factor structures between groups. *British Journal of Mathematical and Statistical Psychology, 27,* 229–239.

Tang, J., Zhang, B., & Xiao, S. (2022). Examining the intention of authorization via apps: Personality traits and expanded privacy calculus perspectives. *Behavioral Sciences (Basel), 12*(7), 218. https://doi.org/10.3390/bs12070218

Tao, S., Liu, Y., & Sun, C. (2024). Examining the inconsistent effect of privacy control on privacy concerns in e-commerce services: The moderating role of privacy experience and risk propensity. *Computers & Security, 140*, 103794. https://doi.org/p7gm

Trakic, A., Karim, R., & Tajuddin, H. H. A. (2023). It is time to recognize the tort of invasion of privacy in Malaysia. *International Data Privacy Law, 13*(4), 299–312. https://doi.org/10.1093/idpl/ipad016

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior, 104,* 106115. *https://doi.org/10.1016/j.chb.2019.08.022*

United Nations. (2025). Child and youth safety online. https://www.un.org/en/global-issues/child-and-youth-safety-online

Valckx, S. (2023). Privacy Paradox: The Relation between Privacy Awareness and Willingness to Disclose. (Master's thesis, Tilburg University, Netherlands). https://arno.uvt.nl/show.cgi?fid=162685

Van der Schyff, K., & Flowerday, S. (2023). The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO. *Computers & Security, 126*, 103071. https://doi.org/10.1016/j.cose.2022.103071

Venkatesh, V., & Davis, F. D. (2000). Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Vespoli, G., Taddei, B., Imbimbo, E. et al. (2024). The concept of privacy in the digital world according to teenagers. *Journal of Public Health*. https://doi.org/p7gn

Xu, H., & Zhang, P. (2025). The influence of anonymity and social ties on personal experience sharing: A comprehensive mixed-methods study. *Proceedings of the ACM on Human-Computer Interaction, 9*(1), GROUP31, 1–22. https://doi.org/10.1145/3701210

Yadav, T., Kala, K., Kolachina, R., Kanneganti, M., & Pasupuleti, S. (2024). Data privacy concerns and their impact on consumer trust in digital marketing. *International Journal of Scientific Research in Engineering and Management, 8*(5), 1–7. https://doi.org/p7gp

Yang, D., Yao, Z., Seering, J., & Kraut, R. (2019, May). The channel matters: Self-disclosure, reciprocity and social support in online cancer support groups. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, *31,* 1-15. ACM. https://doi.org/10.1145/3290605.3300261

Yum, K., & Kim, J. (2024). The influence of perceived value, customer satisfaction, and trust on loyalty in entertainment platforms. *Applied Sciences, 14*(13), 5763. https://doi.org/10.3390/app14135763

Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication, 25*(3), 236–251. https://doi.org/10.1093/jcmc/zmaa004