Journal of Applied Finance & Banking, Vol. 15, No. 1, 2025, 111-131
ISSN: 1792-6580 (print version), 1792-6599(online)
https://doi.org/10.47260/jafb/1516
Scientific Press International Limited

Understanding Self-Disclosure in Social Networking Sites: The Influence of Trust and Perceived Privacy Risk

Cheng-Wen Lee[1] and Yu-Ting Jhou[2]

Abstract

This study investigates the connection between perceived privacy risk and self-disclosure on social networking sites (SNS) through the lens of Privacy Calculus Theory. While SNS platforms offer social benefits, they also pose privacy risks like data breaches. A survey of users of 162 SNS in Taoyuan City, Taiwan, analyzed trust, privacy risk, and self-disclosure using statistical methods. Findings reveal that trust significantly increases self-disclosure, while perceived privacy risk has little impact. Users may downplay privacy concerns or prioritize social engagement. Trust in SNS providers also does not reduce privacy concerns. Older and more educated users perceive higher privacy risks, but gender, marital status, and occupation show no significant effects. Since trust strongly influences self-disclosure, privacy education is essential to raise awareness. SNS providers need to improve privacy settings for enhanced data control. This study helps understand online privacy behavior and emphasizes the importance of educational and platform-based solutions to enhance user security.

JEL classification numbers: D83, L86, M31.
Keywords: Trust, Perceive Privacy Risk, Self-Disclosure, Social Networking Sites.

[1] Department of International Business, College of Business, Chung Yuan Christian University. Taoyuan City, Taiwan.
[2] Ph. D. Program in Business, College of Business, Chung Yuan Christian University. Taoyuan City, Taiwan.

Article Info: *Received:* March 4, 2025. *Revised:* March 18, 2025.
Published online: March 24, 2025.

1. Introduction

Social networking services (SNS), also known as social networking sites, are platforms primarily designed to help users build online communities based on shared interests and activities. These services are typically Internet-based and offer a variety of interactive communication channels, such as email, instant messaging, and multimedia sharing. Social networking sites spread across the Internet through word of mouth, growing from one person to ten, and then to hundreds, similar to the veins of a leaf. These platforms offer users numerous ways to engage with each other, including chatting, sending messages, sharing videos, exchanging files, blogging, and participating in newsgroups. Social networks provide innovative ways for individuals to connect, communicate, and share information. With millions of registered users, these sites have become integral to daily life for many. Some of the most well-known global social networking services include Google+, Myspace, Plurk, Twitter, and Facebook. In mainland China, popular SNS platforms include Renren, QQ Space, Baidu Tieba, and Weibo, among others.

The widespread popularity of social networking sites has prompted numerous studies exploring the concept of self-disclosure on these platforms. Self-disclosure on social networking sites can take many forms, such as sharing photos, posting personal information, updating status feeds, and revealing preferences and experiences. Generally, self-disclosure is recognized as a key factor in developing and maintaining relationships (Laurenceau, et al. 1998) and is essential for conveying trust, which is fundamental to establishing intimacy (Worthy, et al. 1969). Most research on self-disclosure in the context of social networking sites focuses on the issue of personal privacy, examining how users navigate the balance between openness and protecting their personal information.

Social networking sites are online platforms that enable individuals to build social networks, foster relationships, and share common experiences, interests, backgrounds, and real-life connections. However, sharing personal information on these platforms may pose significant privacy risks. The media has reported instances, such as online fraud on Facebook, demonstrating how disclosing personal information can compromise privacy (Vishwanath, 2015). Krasnova, et al. (2010), building on the Privacy Calculus Theory, introduced the concept of cognitive privacy risk in the context of self-disclosure on social networking sites. They argued that cognitive privacy exposure represents the cost associated with the cognitive benefits gained from self-disclosure. Their research further examined the interplay between cognitive costs and privacy risks in influencing individuals' willingness to share personal information online. Therefore, this study primarily investigates how perceived privacy risk impacts self-disclosure behavior on social networking sites.

2. Literature Review

2.1 Development of Social Networking Services

With the emergence of new online social tools like blogs, users started sharing their favorite information on personal homepages across various websites. From 2002 to 2004, the three most popular social networking sites worldwide were Friendster, MySpace, and Bebo. By 2005, MySpace had become the largest social networking platform in the world, with reports indicating that its page views exceeded those of Google, the leading search engine at that time (Ahmad, 2011). In 2006, Facebook opened its website API to third-party developers, allowing the creation of external applications. This crucial move helped Facebook become the fastest-growing website in terms of user base. Inspired by Facebook's success, many other websites began integrating their APIs or supporting third-party developer platforms to enhance their functionality and user engagement.

The rise of social networking sites (SNS) has provided empirical support for the theory of six degrees of separation, which suggests that any individual in the world can be connected to another through a chain of no more than six interpersonal connections. As digital platforms facilitate interactions, people's social circles gradually expand, overlap, and ultimately create vast and complex social networks. Early SNS platforms like Friendster exemplified the principle that "friends of friends are friends," using mutual connections to foster new relationships. However, this model represents only one aspect of social expansion. The scope of SNS goes beyond personal connections, encompassing various forms of community building based on shared interests, experiences, and goals. For instance, platforms like Tieba bring users together around common topics, while sites such as Fexion cater to communities based on specific hobbies.

Educational and alumni networks, such as Facebook and Renren, connect individuals through shared learning experiences. In contrast, professional networking sites like Shangbanzu and Dajie focus on career-oriented interactions. Additionally, social networking service (SNS) platforms can revolve around shared activities (Kwahk and Park, 2016), such as weekend travel experiences, or cater to niche communities, as exemplified by Nongxiang, which facilitates information exchange among Chinese farmers. These diverse examples illustrate that the core purpose of SNS extends beyond merely expanding personal connections; it also involves fostering a wide range of social interactions that enhance collective knowledge-sharing, professional development, and community engagement.

Social networking sites (SNS) provide advanced features and various business models that enhance their growth and profitability. One significant feature is the location check-in function, which enables users to create dedicated pages for discussions on specific topics. The management of these pages is limited to their creators and authorized administrators, ensuring controlled interactions and focused conversations.

Social networking sites (SNS) utilize various business models to generate revenue, each employing different strategies to engage users and maximize profitability. One common model is the advertising revenue model, which earns income through targeted advertisements. This approach uses big data analytics to examine users' login patterns, content preferences, and interaction frequency, allowing platforms to deliver personalized ads. Sites like Kaixin, Renren, Facebook, Mixi, and MySpace effectively take advantage of this model.

In contrast, the user charging model relies on direct payments from users for premium services, as seen with platforms like LinkedIn (Sharone, 2017), which offers professional networking services, and Taiwan's Love Apartment, which provides paid dating services. Another revenue stream, the third-party website inducement model, involves collaborations between SNS platforms and external entities seeking promotion, such as restaurants offering discounts through Facebook ads or political campaigns using the platform for digital outreach and voter engagement. Additionally, the game model integrates in-app purchases within social networking platforms, enabling game developers to earn revenue while sharing profits with the hosting SNS.

This model also offers unique advantages, such as enhancing social connectivity by helping users maintain relationships and reconnect with acquaintances through built-in search tools. Moreover, it provides targeted advertising opportunities, allowing businesses to reach user groups with shared interests directly within gaming environments. Despite these diverse revenue models and their benefits, SNS platforms face critical challenges, particularly in safeguarding user privacy and data security. The extensive collection and analysis of user data for targeted advertising and social engagement raise concerns about privacy breaches and data misuse. Effectively addressing these issues is essential for maintaining user trust and ensuring the long-term sustainability of social networking services.

2.2 Self-Disclosure

2.2.1 Online Self-Disclosure

Researchers have extensively explored the role of self-disclosure in various online environments, building on principles from information and communication technology (ICT) and information technology (IT) (Misoch, 2015). Chou et al. (2009) examined mutual self-disclosure in business-to-consumer (B2C) contexts, finding that increased self-disclosure by companies encouraged consumers to reciprocate with their self-disclosure. Additionally, research has investigated the cognitive and behavioral factors influencing consumers' willingness to disclose personal information online, particularly when interacting with unfamiliar sellers. The concept of online information disclosure is primarily understood through Social Exchange Theory, as proposed by P. M. Blau in 1964 (Kieserling, 2019), and Privacy Calculation Theory, developed by Culnan and Armstrong in 1999. Most studies on this topic view it as a subjective assessment of the costs and benefits associated with an exchange relationship.

Specifically, some scholars argue that privacy compromises are often perceived as an inevitable trade-off for accessing desired online services. Studies on online privacy behavior, such as Malhotra, et al. (2004)**,** have demonstrated that perceived privacy risks negatively influence individuals' willingness to disclose personal information. However, not all users exhibit equal sensitivity to privacy concerns. For example, Hugl (2011) observed that younger users of social networking sites (SNS) tend to be less concerned about privacy risks and advised SNS operators to implement measures to raise awareness of these risks. Despite growing attention to privacy concerns, some users remain relatively indifferent to potential privacy threats, highlighting the complex and multifaceted nature of online self-disclosure. Given these insights, this study aims to explore further the factors that influence self-disclosure behaviors on social networking sites, contributing to a deeper understanding of the motivations, perceptions, and trade-offs that shape users' information-sharing decisions in online social environments.

2.2.2 Self-Disclosure on Social Networking Sites

The widespread popularity of social networking sites (SNS) has prompted numerous studies on self-disclosure behaviors within these platforms. Self-disclosure on SNS can take various forms, including sharing photos, posting personal information, updating status messages, and expressing personal preferences or experiences. Self-disclosure is widely recognized as a critical factor in building and maintaining relationships, as it fosters intimacy and signals trust (Laurenceau, et al. 1998; Worthy, et al. 1969). The majority of research on self-disclosure in SNS contexts has approached the topic from a privacy perspective. For instance, Acquisti and Gross (2006) collected Facebook profile data and found that many users disclosed significant personal information, often due to a lack of understanding of privacy settings.

Similarly, Dwyer, et al. (2007) investigated the impact of trust and privacy concerns on Facebook users' self-disclosure behaviors, highlighting the role of perceived safety and platform transparency. Expanding on these findings, Hugl (2011) conducted a comprehensive literature review on privacy issues and SNS, revealing that adult users exhibit heightened concern about privacy threats and cautioning that single-dimensional privacy frameworks fail to capture the complexities of online privacy. Additionally, Xu, et al. (2022), discovered that while privacy concerns exist, they do not necessarily deter users from engaging with SNS, suggesting that other factors, such as social rewards and platform design, may outweigh privacy apprehensions. Together, these studies highlight the complex interplay between privacy, trust, and self-disclosure behaviors on social networking sites, emphasizing the need for further exploration of the factors influencing users' decisions to share personal information in online social contexts.

2.2.3 Cognitive Benefits of Self-Disclosure on Social Networking Sites

Previous literature has identified four key cognitive benefits associated with the use of social networking sites (SNS): maintaining the legitimacy of existing relationships**,** establishing new relationships**,** self-expression**,** and enjoyment (Krasnova, et al. 2010). These benefits highlight the diverse psychological and social motivations that drive user engagement on SNS platforms. Maintaining existing relationships involves sustaining social ties and reinforcing connections with friends, family, and acquaintances. Establishing new relationships refers to expanding one's social network by connecting with new individuals, and fostering opportunities for social and professional growth. Self-expression encompasses sharing personal opinions, experiences, and creative content, allowing users to construct and present their digital identities. Lastly, enjoyment reflects the intrinsic satisfaction and pleasure derived from interacting with others, engaging with content, and participating in social activities within online communities. Together, these cognitive benefits contribute to the widespread adoption and sustained use of social networking platforms.

2.2.4 Cost Mitigation Factors of Self-Disclosure on Social Networking Sites

Despite being aware of privacy risks, many users continue to share personal information on social networking sites (SNS). This discrepancy can be attributed to users' trust in both the service providers and fellow platform members (Acquisti and Gross, 2006). Additionally, users rely on privacy control mechanisms provided by SNS platforms to manage access to their personal information. A primary source of uncertainty for SNS users is whether the platform providers can effectively monitor and protect their personal data. According to Social Exchange Theory, trust reduces privacy-related uncertainties and encourages users to participate in online interactions (Metzger, 2004). Trust is essential for mitigating perceived risks, as users are more likely to engage in self-disclosure when they believe service providers are benevolent, honest, and reliable (Cheung and Lee, 2006). When users perceive that SNS providers demonstrate care, honesty, and consistency in their privacy practices, they are less concerned about privacy risks and are more willing to share personal information. Conversely, a loss of trust in service providers increases perceived privacy risks and diminishes self-disclosure (Hill, 2012). This issue is particularly evident in the context of Facebook**,** where data privacy controversies have heightened user concerns about information security. Such instances highlight how perceived failures in data protection can erode trust and subsequently reduce users' willingness to share personal information.

In addition to trust in platform providers, trust among members of the social networking community significantly influences self-disclosure behaviors. SNS platforms store vast amounts of user-generated content, including profiles, photos, and online activities, which are easily accessible to other users (Chen, et al. 2016). Since users are generally unable to monitor the behavior of other members due to time and technical constraints, they must trust that their peers will not misuse the

disclosed information. Krasnova, et al. (2010) highlight that cognitive similarity between users fosters trust within the social network, as shared interests and values contribute to a sense of community and mutual respect. Additionally, Culnan and Armstrong (1999) argue that users' ability to control their personal information reduces perceived privacy risks and enhances trust. This assertion is further supported by Xu, et al. (2022), who found that privacy self-control mechanisms, such as customizable privacy settings, significantly lower users' perceived privacy risks, and demonstrated that when consumers can control their personal information, their trust in online sellers increases.

Moreover, Krasnova et al. (2010) emphasized that privacy control mechanisms provided by service providers are critical for building trust within SNS communities. Control features, such as adjustable privacy settings and audience selectors, empower users to manage their information visibility and reinforce their confidence in the platform. Within SNS environments, users typically regard their online connections as "friends," which grants those connections access to personal profiles, updates, and shared content. Consequently, the perception of mutual trust among peers reduces privacy concerns and fosters greater self-disclosure on social networking sites. Therefore, this paper aims to explore the relationship between trust, perceived privacy risk, and self-disclosure**,** examining how these factors interact and influence individuals' willingness to share personal information.

3. Research Method

3.1 Questionnaire Design

The questionnaire scale used in this study was developed by translating and adapting items from the trust measurement scale presented in the research by Cheung (2015)**,** which focused on exploring the concept of trust. The finalized questionnaire comprises 15 items**,** as detailed in Table 1**.** A five-point Likert scale was employed for measurement, with response options ranging from 1 (Strongly Disagree) to 5 (Strongly Agree)**.** The scale captures varying degrees of agreement, including Strongly Disagree**,** Disagree**,** Neutral**,** Agree**,** and Strongly Agree**,** allowing for a comprehensive assessment of participants' perceptions of trust.

Table 1: Questionnaire Design

Facets	Question Items
Trust	1. Facebook is open and accepting of the needs of community members. 2. Facebook conducts credible activities to show that community members care about issues. 3. Facebook also cares about the happiness of its community members. 4. Facebook is honest in its dealings with community members. 5. Facebook remains committed to its community members. 6. Facebook is trustworthy. 7. Other Facebook members have done their best to help me. 8. Other Facebook members care about the happiness of others. 9. Other Facebook members openly and accept mutual needs. 10. Other Facebook members were honest in their dealings with one another. 11. Other Facebook members maintained their commitment. 12. Other Facebook members are trustworthy.
Perceived Privacy Risks	1. Overall, I find that posting personal information on social networking sites is risky. 2. Please evaluate your awareness of privacy risks when using social networking sites.
Self-Disclosure	1. I have a complete profile and information on Facebook 2. I will take the time to update my profile. 3. I keep my friends able to see my profile and messages on Facebook 4. Sometimes when I want to talk about something, I can share it through Facebook.

3.2 Data Collection

After establishing the analytical matrix, this study selected social networking site users in Taoyuan City, Taiwan, as the primary sample group. The target population comprises individuals who actively use social networking platforms. To collect data, the study employed a convenience sampling method, which was chosen due to constraints related to time, manpower, and research costs. Convenience sampling was deemed appropriate for its practicality, enabling researchers to efficiently reach participants who were readily accessible and willing to participate. Given the confirmatory nature of this study, the sample size was determined based on the research design and analytical requirements. A total of 162 valid questionnaires were collected from respondents, with each questionnaire thoroughly reviewed to ensure completeness and validity before being included in the analysis. Although the sample size was relatively small, it was deemed sufficient for confirmatory analysis, as the primary objective of the study was to validate the proposed model and test the research hypotheses.

3.3 Reliability Test

This study employed correlation analysis and Cronbach's α coefficient analysis as the primary criteria for selecting scale items. The item selection process was guided by two principles: first, items were excluded if their corrected item-total correlation with the respective subscale did not reach the 0.01 significance level; second, items were removed if their exclusion increased the overall Cronbach's α coefficient. Reliability, in the context of this study, refers to the degree of consistency and stability in measurement results. It represents the extent to which a measurement procedure yields consistent outcomes when applied to the same or similar phenomena across different conditions or points in time. The observed score in any measurement comprises two components: the true score and the error score. Higher reliability is indicative of lower measurement error, thereby ensuring that observed values remain stable and consistent over time, irrespective of variations in form or administration. To assess the internal consistency of items within the same construct, this study utilized Cronbach's α coefficient, a widely recognized measure of reliability. A higher Cronbach's α value indicates stronger internal consistency, reflecting the extent to which items within a scale measure the same underlying construct.

Nunnally (1978) recommended a Cronbach's alpha (α) coefficient of at least 0.70 for general research reliability. Similarly, Roberts and Wortzel (1979) stated that a Cronbach's alpha above 0.60 indicates acceptable reliability. This study evaluated the questionnaire's reliability through internal consistency, with higher α values reflecting stronger reliability. Table 2 presents the results for the trust, perceived privacy risk, and self-disclosure scales. The Cronbach's alpha values were 0.891 for trust and 0.858 for self-disclosure, both exceeding the 0.60 benchmark. These results demonstrate that the scales used in this study exhibit strong internal consistency and acceptable reliability.

Table 2: Reliability Test

Variable	Number of Questions	Cronbach's alpha coefficient
Trust	12	0.833
Perceived privacy risks	2	0.891
Self-disclosure	4	0.858

4. Result and Analysis

4.1 Demographic Profile of the Sample

Structured questions are commonly used in quantitative research methodologies to collect data. In recent years, online data collection has gained popularity among educational researchers due to its efficiency and convenience. Although still underutilized for this purpose, it offers a viable alternative to traditional data collection methods. To gather a large number of responses and ensure easy access to valid samples, we conducted a survey using an electronic questionnaire. Between October and November 2023, we distributed 300 questionnaires via Google Forms, sharing the link through LINE, WhatsApp, and personal networks, including friends and family. A total of 169 responses were deemed valid for analysis.

Table 3 presents a detailed demographic profile of the study sample, outlining the distribution of respondents across five key variables: gender, age, education level, profession, and marital status. Understanding these demographic characteristics is essential for evaluating the representativeness of the sample and identifying potential biases that may influence the study's findings. The sample is predominantly female, with women comprising 69.2% of the total participants. This gender imbalance may have significant implications, particularly if the research topic involves factors that are influenced by gender, such as workplace dynamics, health-related behaviors, or financial decision-making.

The majority of respondents (84%) are aged 31 years and older, with the highest concentration in the over 41 years category (43.8%). The underrepresentation of younger individuals (only 16%) suggests that the sample is primarily composed of mature adults who may have more stable career trajectories, higher financial security, and established lifestyle patterns. This could influence responses to questions regarding economic stability, consumer behavior, and long-term planning.

Table 3: Demographic Profile of the Sample

	Characteristics	Number	Percentage (%)
Gender	Male	52	30.8
	Female	117	69.2
Age	Under 25 years old	11	6.5
	26-30 years old	16	9.5
	31-40 years old	68	40.2
	Over 41 years old	74	43.8
Education	High school	25	14.8
	College	70	41.4
	Graduate School or above	74	43.8
Occupation	Student	48	28.4
	Freelance	24	14.2
	Military, Civil Service and Education	31	18.3
	Industry and Commerce	32	18.9
	Medical Industry	10	5.9
	Insurance	12	7.1
	Others	12	7.1
Marital status	Unmarried	106	62.7
	Married	63	37.3

The majority (85.2%) of respondents have attained at least a college-level education, with a significant proportion (43.8%) holding graduate or postgraduate degrees. The high level of education among respondents suggests that their cognitive processing, problem-solving abilities, and decision-making patterns may differ from those of the general population, particularly in studies involving financial literacy, technology adoption, or policy awareness. Responses may skew towards an academic or professional perspective, potentially overlooking insights from lower-education groups that may have different social, economic, and behavioral patterns. The highest proportion of respondents (28.4%) are students, followed by those engaged in industry, commerce, and civil service (over 37%). Certain professional sectors, such as medical (5.9%) and insurance (7.1%), are underrepresented. The high percentage of students suggests that the sample may reflect a learning-oriented perspective, with potential biases towards academic viewpoints, digital literacy, and aspirational career trajectories. The low representation of medical and insurance professionals may limit the applicability of the findings to healthcare and financial

industries, especially if the research involves themes like health behaviors, financial planning, or risk assessment.

A significant majority of respondents (62.7%) are unmarried, suggesting that perspectives in the study may be more aligned with individual decision-making rather than family-oriented considerations. If the research involves financial behavior, consumption patterns, or lifestyle choices, these findings might more reflect single individuals rather than those making household-based decisions.

4.2 T-Test and One-Way ANOVA

A one-way analysis of variance (ANOVA) is a statistical method used to determine whether there are significant differences among the means of three or more independent groups. In contrast, an independent samples t-test assesses differences between the means of two independent groups. In this study, one-way ANOVA was utilized to examine variations in key variables across different demographic factors, including age, education, and profession. Meanwhile, t-tests were conducted to analyze differences in trust, perceived privacy risk, and self-disclosure based on gender and marital status. If the results indicated statistical significance at $p < 0.05$, Scheffé's test and the Least Significant Difference (LSD) test were applied as post hoc analyses to further explore group differences and identify any significant relationships across levels.

4.2.1 Gender

This study employs the t-test to examine differences in trust, perceived privacy, and self-disclosure between respondents of different genders. The statistical results, presented in Table 4**,** indicate that no statistically significant differences were observed across these variables. This suggests that trust, perceived privacy risk, and self-disclosure do not significantly differ between male and female respondents.

Table 4: T-Test of Gender

Variable name	Gender	Mean	Standard Deviation	t-value	p-value
Trust	Male	3.3129	0.4113	2.147	0.899
	Female	3.1202	0.5031		
Perceived Privacy Risks	Male	3.6316	0.4667	0.066	0.151
	Female	3.6744	0.6536		
Self-Disclosure	Male	2.7895	1.0969	0.191	0.666
	Female	2.6802	0.8116		

4.2.2 Marital Status

This study employs an independent samples t-test to examine differences in trust, perceived privacy, and self-disclosure among respondents with different marital If statuses**.** The statistical analysis results are presented in Table 5**.** As shown in the table, no statistically significant differences were observed across these variables at any level. This indicates that trust, perceived privacy, and self-disclosure do not vary significantly based on marital status**.**

Table 5: T-Test of Marital Status

Variable	Marital Status	Mean	Standard Deviation	t-value	p-value
Trust	Unmarried	3.2108	0.5174	0.448	0.506
	Married	3.1256	0.4202		
Perceived Privacy Risk	Unmarried	3.6667	0.5541	0.008	0.928
	Married	3.6522	0.6815		
Self-Disclosure	Unmarried	2.8141	0.8146	1.313	0.256
	Married	2.5435	1.0271		

4.2.3 Age

This study employs one-way ANOVO to examine differences in trust, perceived privacy risk, and self-disclosure among respondents of varying age groups. The results of the statistical analysis are presented in Table 6. From the table, it is evident that trust and self-disclosure do not exhibit significant differences across age groups, suggesting that respondents of different ages share similar levels of trust and self-disclosure. However, significant differences are observed in perceived privacy risk among different age groups. Specifically, respondents aged 31-40 perceive higher privacy risks compared to those under 25 years old, with the difference being statistically significant at $p < 0.05$.

Table 6: One-Way ANOVA Analysis of Age

Variable	Age	Mean	Standard Deviation	F -value	p-value	Scheffé's test
Trust	Under 25 years old	2.7361	0.3696	1.348	0.268	
	26-30 years old	3.1852	0.2975			
	31-40 years old	3.2533	0.4654			
	Over 41 years old	3.1749	0.5259			
Perceived Privacy Risk	Under 25 years old	2.8750	0.6292	5.518	0.002	C>A
	26-30 years old	3.3333	0.4083			
	31-40 years old	3.9200	0.5339			
	Over 41 years old	3.6111	0.5605			
Self-disclosure	Under 25 years old	1.8750	1.4361	1.624	0.194	
	26-30 years old	2.7917	0.5792			
	31-40 years old	2.9000	0.9157			
	Over 41 years old	2.6481	0.8241			

Note: A. Under 25 years old, B. 26-30 years old, C. 31-40 years old, D. Over 41 years old

4.2.4 Education

Table 7 presents the one-way ANOVA-test results comparing participants' trust, perceived privacy risk, and self-disclosure across different educational levels. The analysis shows that respondents with a graduate degree or higher perceive significantly greater privacy risks than those with a college degree or lower ($p < 0.05$). In contrast, there were no statistically significant differences in trust or self-disclosure between these educational groups.

Table 7: One-Way ANOVA Analysis of Education

Variable	Education	Mean	Standard Deviation	F -value	p-value	Scheffé's test
Trust	High School	3.7361	0.3555	0.300	0.863	
	College	3.1667	0.4675			
	Graduate School or Above	3.1883	0.4984			
Perceived Privacy Risk	High School	2.8750	0.4392	5.333	0.024	C>A
	College	3.4165	0.5463			
	Graduate School or Above	3.8056	0.6009			
Self-disclosure	High School	2.7750	1.1361	0.639	0.427	
	College	2.6058	0.9596			
	Graduate School or Above	2.7919	0.8609			

Note: A. High School, B. College, C. Graduate School or Above

4.2.5 Occupation

This study employed a one-way ANOVA test to examine potential differences in trust, perceived privacy, and self-disclosure across various occupational groups. As presented in Table 8, while some degree of variation was observed among the groups, these differences did not reach statistical significance ($p > 0.05$). This indicates that individuals from different occupational backgrounds generally exhibit comparable levels of trust, perceived privacy, and self-disclosure. The lack of significant differences suggests that occupational background may not play a critical role in shaping these psychological and behavioral constructs. One possible explanation is that factors such as individual personality traits, prior experiences, or broader cultural influences may exert a stronger impact than professional roles. Additionally, occupational groups may share similar experiences regarding privacy concerns and self-disclosure in the context under investigation, reducing the likelihood of substantial variation.

Table 8: One-Way ANOVA Analysis of Occupation

Variable	Profession	Mean	Standard Deviation	F -value	p-value	Scheffé's test
Trust	Student	3.7341	0.3696	0.292	0.268	
	Freelance	3.2531	0.5768			
	Military, Civil Service and Education	3.1486	0.4464			
	Industry and Commerce	3.1667	0.4438			
	Medical Industry	3.2634	0.5652			
	Insurance	3.7749	0.4525			
	Others	3.1749	0.5259			
Perceived Privacy Risk	Student	2.8750	0.6292	5.518	0.123	
	Freelance	3.4772	0.4363			
	Military, Civil Service and Education	3.7209	0.6390			
	Industry and Commerce		0.7521			
	Medical Industry	4.5000	0.6541			
	Insurance	3.9210	0.4551			
	Others	3.3335	0.5339			
Self-disclosure	Student	2.8750	1.4361	1.624	0.998	
	Freelance	3.1750	0.9516			
	Military, Civil Service and Education	3.2201	0.9013			
	Industry and Commerce	3.2317	0.4792			
	Medical Industry	3.2152	0.7551			
	Insurance	3.1522	0.7157			
	Others	3.6481	0.8221			

From a practical standpoint, this finding has important implications for organizations and policymakers. Since occupational background does not appear to significantly influence trust, privacy perceptions, or self-disclosure, interventions aimed at enhancing trust and privacy awareness should consider broader, cross-occupational strategies rather than tailoring efforts to specific professional groups. Furthermore, in contexts such as online interactions, workplace environments, and digital communication, organizations may need to focus on universal factors—such as transparency, security policies, and communication strategies—rather than assuming that occupational differences inherently shape these attitudes and behaviors. Future research could explore other potential moderators, such as industry-specific norms, technological exposure, or demographic factors, to further clarify the determinants of trust, privacy concerns, and self-disclosure.

4.3 Pearson Correlation Coefficient

Correlation is a statistical concept that measures the degree to which two variables move in relation to each other. It provides insight into the strength and direction of a relationship between two continuous variables. Correlation does not imply causation but rather quantifies the association between variables. The Pearson Correlation Coefficient (denoted as *r*) developed by Karl Pearson in the late 19th century, is the most commonly used correlation measure in statistics. It evaluates the linear relationship between two continuous variables. It is widely used in various fields such as economics, finance, psychology, biology, and social sciences. The Pearson correlation coefficient measures only linear relationships. If the relationship between two variables is non-linear, Pearson's *r* may be misleading. For instance, a quadratic relationship may show a near-zero Pearson correlation despite a strong association. The Pearson correlation coefficient is defined as Equation (1):

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2} \cdot \sqrt{\sum(Y_i - \bar{Y})^2}} \tag{1}$$

Table 9: The Analysis of Pearson Correlation Coefficient

	Mean	S.D.	Trust	Perceived Privacy Risk	Self-Disclosure
Trust	3.1048	0.6368	1		
Perceived Privacy Risk	3.6613	0.5850	0.173	1	
Self-Disclosure	2.7137	0.9221	0.245	0.050	1

The relationship between trust, perceived privacy risk, and self-disclosure suggests that trust plays a key role in influencing self-disclosure. The positive correlation (0.245) between trust and self-disclosure indicates that individuals who have higher trust are more likely to disclose personal information. Meanwhile, perceived privacy risk has a weak positive correlation (0.050) with self-disclosure, suggesting that concerns about privacy risks do not significantly deter individuals from sharing information. Additionally, the weak correlation (0.173) between trust and perceived privacy risk implies that as trust increases, perceived privacy risks may slightly increase, possibly because individuals who are more trusting still recognize potential privacy risks but choose to engage in self-disclosure despite them. Overall, trust appears to be the strongest factor influencing self-disclosure, while perceived privacy risk has minimal impact.

4.4 Regression Coefficient Analysis

Regression analysis is a statistical method used to examine the relationship between dependent and independent variables. The regression coefficient quantifies the strength and direction of this relationship. In a regression equation, the regression coefficient (β) represents how much Y changes for a one-unit increase in X, assuming other variables remain constant as shown in Equation (2).

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_n X_n + \varepsilon \tag{2}$$

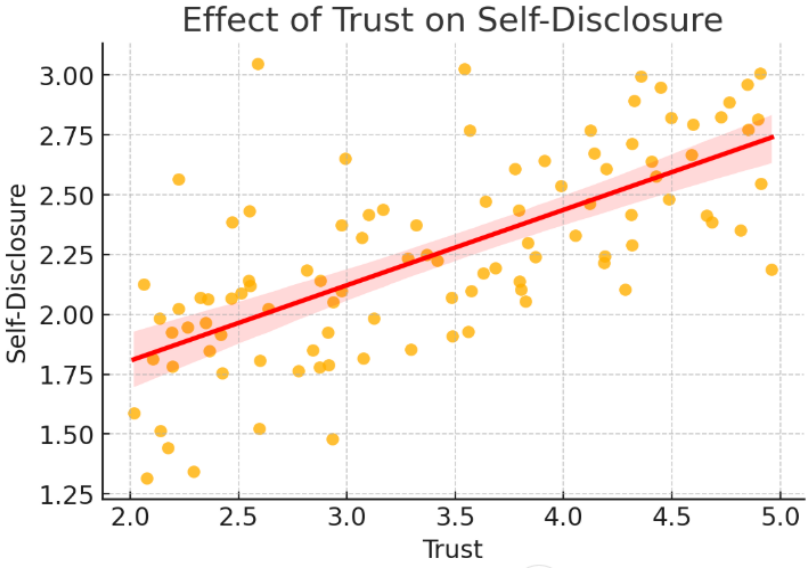

Figure 1: The Effect of Trust on Self-Disclosure

From Figure 1, the scatterplot illustrates the relationship between trust and **s**elf-disclosure, with individual data points representing observations. A red regression line is included, indicating a positive correlation between these two variables, suggesting that as levels of trust increase, individuals tend to engage in greater self-disclosure. This relationship aligns with theoretical expectations, as trust is often considered a fundamental prerequisite for open and honest communication. Additionally, the shaded region around the regression line represents the 95% confidence interval**,** which estimates the range within which the true regression line is likely to fall. A narrower confidence interval suggests greater precision in the estimated relationship, while a wider interval indicates more variability in the data. This visualization underscores the statistical significance and reliability of the observed association between trust and self-disclosure, supporting the notion that trust fosters a greater willingness to share personal information.

From Figure 2, the bar chart presents the standardized regression coefficients (β values) for the predictors of **s**elf-disclosure, visually illustrating the relative strength and direction of their effects. The blue bar, representing trust (β = 0.35), indicates a moderate to strong positive effect, suggesting that higher levels of trust are associated with significantly greater self-disclosure. This finding aligns with existing literature, emphasizing trust as a key determinant in individuals' willingness to share personal information. Conversely, the red bar, corresponding to Perceived Privacy Risk (β = -0.05), exhibits a very small negative effect, indicating that concerns about privacy risks have minimal influence on self-disclosure. The near-zero coefficient suggests that while privacy concerns may theoretically discourage disclosure, their actual impact in this context is negligible. The comparison of these coefficients highlights trust as a more influential factor in predicting self-disclosure, while perceived privacy risk does not appear to significantly deter individuals from sharing information

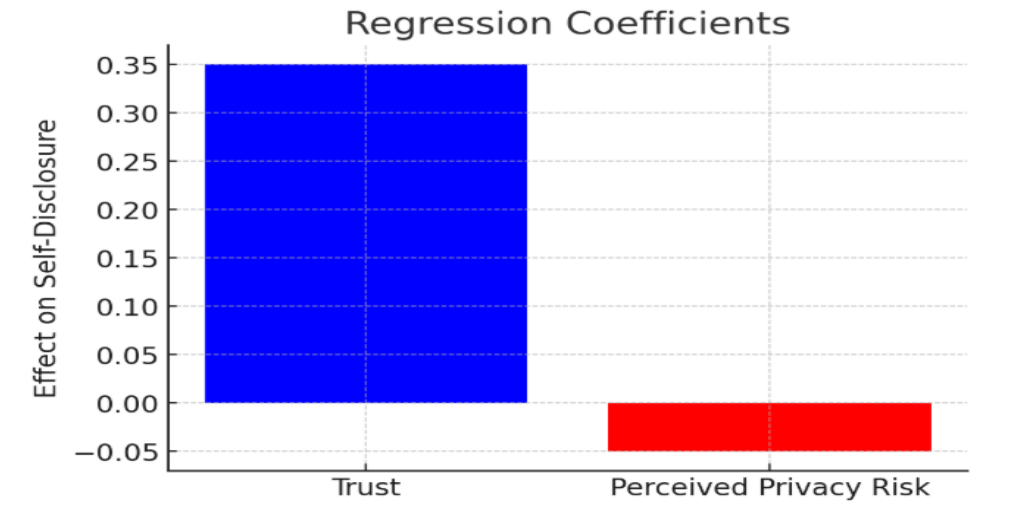

Figure 2: Regression Coefficients of Trust and Perceived Privacy Risk on Self-Disclosure

The regression analysis suggests that trust is a significant predictor of self-disclosure, while perceived privacy risk has little to no impact**.** This implies that people tend to disclose personal information based on how much they trust the environment, rather than how risky they perceive it to be.

5. Conclusion and Suggestion

This study examines the relationship between perceived privacy risk and self-disclosure behavior on social networking sites (SNS) within the framework of Privacy Calculus Theory. The increasing popularity of SNS platforms such as Facebook and Twitter has raised concerns about the risks associated with sharing personal information online. While users benefit from social connectivity, self-expression, and relationship building, they also face significant privacy risks, including data breaches and online fraud. The study aims to determine how users weigh these benefits against potential privacy concerns and how trust influences their self-disclosure behavior.

A quantitative approach was employed, utilizing a structured survey administered to SNS users in Taoyuan City, Taiwan. A total of 162 valid responses were collected and analyzed using statistical methods, including t-tests, one-way ANOVA, correlation analysis, and regression analysis. The study assessed three key variables: trust, perceived privacy risk, and self-disclosure. Trust was further categorized into trust in SNS service providers and trust among SNS community members.

The findings indicate that trust plays a significant role in self-disclosure behavior. A strong positive correlation was observed between trust and self-disclosure, suggesting that individuals who perceive SNS platforms as trustworthy are more likely to share personal information. However, contrary to expectations, perceived privacy risk did not have a significant impact on self-disclosure. This implies that users may either underestimate privacy risks or prioritize the social benefits of SNS engagement over potential threats. Additionally, trust in SNS service providers did not significantly influence perceived privacy risk, indicating that users do not necessarily associate platform credibility with lower privacy concerns.

Demographic analyses revealed that perceived privacy risk varied across age and education levels. Specifically, older users (aged 31-40) and those with graduate-level education exhibited higher concerns regarding privacy risks. However, gender, marital status, and occupational background did not significantly influence trust, privacy risk perception, or self-disclosure behavior.

Regression analysis further supported the direct impact of trust on self-disclosure, while perceived privacy risk remained statistically insignificant. This finding challenges the assumption that heightened awareness of privacy risks leads to reduced information sharing. Instead, users appear to rely on trust—whether in the platform or in their online connections—when deciding to disclose personal details.

The study has significant implications for both SNS users and platform providers. Given that perceived privacy risks do not deter self-disclosure, there is a pressing

need for enhanced privacy education. Users should be made more aware of potential risks through targeted awareness campaigns. Additionally, SNS providers should simplify privacy settings, enabling users to better manage their data and improve overall platform security.

In conclusion, this research contributes to the understanding of self-disclosure behavior in online environments by highlighting the predominant role of trust over privacy risk concerns. The results suggest that trust is a critical factor in shaping user behavior on SNS, while privacy concerns alone are insufficient to influence disclosure decisions. Future studies should further explore other psychological and contextual factors that may moderate the relationship between privacy risk perception and self-disclosure behavior.

Social networking sites are online platforms that enable individuals to build social networks and foster relationships while sharing experiences, interests, and backgrounds. However, when users share personal information on these sites, they face risks concerning their privacy. Media reports have highlighted instances, such as online fraud, that demonstrate how sharing personal details on platforms like Facebook can compromise privacy.

This study concludes that perceived privacy risks do not significantly affect the likelihood of self-disclosure on social networking sites. This indicates that users often do not consider potential privacy threats when deciding to share personal information. Therefore, education experts recommend implementing programs to inform users about the privacy risks associated with self-disclosure on these platforms. Additionally, social networking service providers should develop clear privacy indicators to communicate the level of privacy protection available to users.

References

[1] Acquisti, A. and Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In International Workshop on Privacy Enhancing Technologies (pp. 36-58). Berlin, Heidelberg: Springer Berlin Heidelberg.

[2] Ahmad, A. (2011). Social network sites and its popularity. International Journal of Research and Reviews in Computer Science, 2(2), 522.

[3] Chen, X., Pan, Y., and Guo, B. (2016). The influence of personality traits and social networks on the self-disclosure behavior of social network site users. Internet Research, 26(3), 566-586.

[4] Cheung, C. M. and Lee, M. K. (2006). Understanding consumer trust in Internet shopping: A multidisciplinary approach. Journal of the American Society for Information Science and Technology, 57(4), 479-492.

[5] Cheung, M. W. L. (2015). Meta-analysis: A Structural Equation Modeling Approach. John Wiley & Sons.

[6] Chou, W. Y. S., Hunt, Y. M., Beckjord, E. B., Moser, R. P., and Hesse, B. W. (2009). Social media use in the United States: implications for health communication. Journal of Medical Internet Research, 11(4), e1249.

[7] Culnan, M. J. and Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104-115.
[8] Dwyer, C., Hiltz, S., and Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. AMCIS 2007 Proceedings, 339.
[9] Hill, C. E. (2012). Consensual Qualitative Research: A Practical Resource for Investigating Social Science Phenomena. American Psychological Association.
[10] Hugl, U. (2011). Reviewing Person's value of privacy of online social networking. Internet Research, 21(4), 384-407.
[11] Kieserling, A. (2019). Blau (1964): exchange and power in social life. Schlüsselwerke der Netzwerkforschung, 51-54.
[12] Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of Information Technology, 25(2), 109-125.
[13] Kwahk, K. Y. and Park, D. H. (2016). The effects of network sharing on knowledge-sharing activities and job performance in enterprise social media environments. Computers in Human Behavior, 55, 826-839.
[14] Laurenceau, J. P., Barrett, L. F., and Pietromonaco, P. R. (1998). Intimacy as an interpersonal process: the importance of self-disclosure, partner disclosure, and perceived partner responsiveness in interpersonal exchanges. Journal of personality and social psychology, 74(5), 1238.
[15] Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355.
[16] Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. Journal of Computer-Mediated Communication, 9(4), JCMC942.
[17] Misoch, S. (2015). Stranger on the internet: Online self-disclosure and the role of visual anonymity. Computers in Human Behavior, 48, 535-541.
[18] Nunnally, J. C. (1978). An overview of psychological measurement. Clinical Diagnosis of Mental Disorders: A Handbook, 97-146.
[19] Roberts, M. L. and Wortzel, L. H. (1979). New life-style determinants of women's food shopping behavior. Journal of Marketing, 43(3), 28-39.
[20] Sharone, O. (2017). LinkedIn or LinkedOut? How social networking sites are reshaping the labor market. In Emerging Conceptions of Work, Management and the Labor Market (Vol. 30, pp. 1-31). Emerald Publishing Limited.
[21] Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. Journal of Computer-Mediated Communication, 20(1), 83-98.
[22] Worthy, M., Gary, A. L., and Kahn, G. M. (1969). Self-disclosure as an exchange process. Journal of Personality and Social Psychology, 13(1), 59.
[23] Xu, H., Phan, T. Q., and Tan, B. C. (2022). Why are people addicted to SNS? Understanding the role of SNS characteristics in the formation of SNS addiction. Journal of the Association for Information Systems, 23(3), 806-837.