Luz y Saber
The Official Research Scholarly Journal of
Colegio de San Juan de Letran – Manila
Volume 18 Issue 1
EISSN: 2244-6338



# SOCIAL MEDIA USERS' RISK PERCEPTION, AWARENESS, AND BEHAVIOR TOWARDS PRIVACY AMONG STUDENTS OF A PRIVATE COLLEGE

Maria Luisa M. Carlos, Cristina D. delos Santos, Ramon S. Olaez III, Winchell B. Palomeno
Faculty Member, College of Engineering and Information Technology

## ABSTRACT

Social media connects people in today's society; however, its large user base is vulnerable to security threats. This study explores the relationship between perceived privacy risks, awareness, and protection behavior. A face-to-face survey conducted in March 2023 examined socio-demographics, social media use, risk perception, privacy awareness, and protection behaviors. Using Pearson correlation, the study found a strong link between perceived risk and protective actions, as well as between privacy awareness and behavior. Among 332 stratified random participants, most were female students aged 20–22. The results suggest that respondents are highly aware of privacy risks and actively take steps to protect their personal data. These findings highlight the need for educational institutions to implement social media privacy awareness training programs to reinforce safe practices and safeguard student information online.

**Keywords**: social media, privacy risk, privacy awareness, privacy protection behavior

## INTRODUCTION

Social media is a popular communication tool among students, who frequently use platforms like Facebook, Twitter, and YouTube. As of January 2023, there were approximately 4.76 billion social media users worldwide (Statista). Facebook remains the leading platform, with around 2.9 billion active users. In the Philippines, about 30.5% of Facebook users were aged 18 to 25 as of December 2022. With 84.07 million digital users recorded in January 2022, the country ranked ninth globally. Owing to its exceptionally high engagement rates, the Philippines has often been referred to as the "social media capital of the world."

Social media platforms (SMPs) allow individuals to interact, share experiences, and explore their environment, reducing communication barriers (Bishop, 2019; Oducado et al., 2019). While social media has become integral to daily life, privacy breaches have also risen (Tao et al., 2019; Jozani, 2020). Notable breaches include 700 million LinkedIn users' data leaked in June 2021, 500 million records scraped by a "God User," and Facebook's 2021 breach exposing 533 million users' data (Hill & Swinhoe, 2022). These incidents highlight growing privacy risks linked to widespread social media use.

Users of SMPs often share personal data due to high trust levels. This trust is exploited by attackers who collect data for malicious purposes, posing major privacy and security risks (Kayes & Iamnitchenko, 2017). Cyberattacks and data breaches can cause serious harm. Despite awareness of these risks, users frequently trade privacy for online services. It is essential for users to understand these dangers and take protective measures when storing information online.

This study examines students' risk perceptions, awareness, and privacy protection behaviors in relation to their use of social media. The research findings could aid educational institutions in providing comprehensive education on privacy to students. Also, this study could influence the privacy protection strategies individuals utilize on SMPs.

### Theoretical framework

#### Theory of Ritualized Media Use

The Theory of Ritualized Media Use (TRMU) suggests media consumption goes beyond information or entertainment, becoming part of daily routines for relaxation and social interaction (Barth et al., 2017; Rubin, 1984). Rituals include scheduled viewing or casually flipping through channels (Strecker et al., 2015). Similarly, social media use becomes habitual, increasing engagement (Hossain, 2019). However, repeated use may lead to personal information disclosure and privacy risks. Users must be cautious and weigh the benefits and risks before sharing personal data online (Schmidt et al., 2022).

This theory provides additional insight into the tremendous popularity of SMPs such as Facebook and their apparent disregard for users' privacy.

#### Uses and gratification theory

The uses and gratifications theory explains that individuals choose media based on personal needs. Social media use is driven by desired gratifications, influenced by user traits like age, gender, and personality (Katz et al., 1973; Olpin et al., 2023; Kircaburun, 2020).

Social media use differs by platform, driven by personal choice and gratification. Users engage for various reasons, including building relationships, seeking information, leisure, comfort, self-enhancement, monitoring others, and social interaction (Masciantonio & Bourguignon, 2023; Falgoust et al., 2022; Hossain, 2019; Alhabash & Ma, 2017). Preferences reflect individual autonomy and motivations behind media engagement.

#### Protection Motivation Theory

Protection motivation theory (PMT) explains protective behavior through four fear appeal components: severity, likelihood, response effectiveness, and self-efficacy (Maddux & Rogers, 1983). It focuses on threat and coping appraisal-assessing danger and vulnerability, and the ability to manage threats. People valuing privacy often take more protective actions (Baruh et al., 2017; Büchi et al., 2017).

The theory offers a framework for describing individuals' risk perception and their ability to defend against potential threats instead of highlighting the motives for disclosing or not disclosing private information. The use of PMT in the realm of privacy demonstrates how perceptions may impact people's actions.

### Literature review

#### Perceived privacy risk

People often feel uncertain when faced with ambiguity. Slovic (2000) defines risk perception as a subjective interpretation shaped by knowledge and confidence. In social media, privacy risk refers to threats users face when sharing personal data. Many users overlook these risks, especially those with limited internet knowledge (Alguliyev et al., 2018; Kayes & Iamnitchi, 2017). While privacy settings offer some control, they do not ensure full protection (Office of

the Privacy Commissioner of Canada, 2019). This study examines whether users perceive privacy risks when using SMPs.

**Privacy awareness**

Privacy awareness involves understanding how personal data is protected, its presence online, and its future implications (Correia & Compeau, 2017). The National Privacy Commission (2022) stresses its importance in fostering a privacy-conscious culture in the Philippines. A lack of awareness may expose users to cyberattacks (Jain et al., 2021). Since social media collects vast data, users must understand how it's gathered and shared, adjust privacy settings, and be cautious when sharing information (Lee & Attablayo, 2023).

This issue prompted us to investigate consumers' awareness of privacy factors such as social sharing visibility, information sharing with third parties, privacy settings, and security measures on social media sites.

**Visibility of profile information**

Visibility refers to how much personal content is seen by others (Limecube, 2022). Limiting visibility to selected individuals helps protect horizontal privacy but may not fully safeguard vertical privacy, as platforms or third parties can still access and use the data (Bartsch & Dienlin, 2016; Quinn & Epstein, 2018).

**Privacy settings**

Social media platforms have default privacy settings that users should adjust before posting. These settings help limit interactions with specific followers (Monti & Wacks, 2019). However, they can be confusing, leading most users to stick with defaults (Fiesler et al., 2017). Privacy-conscious users must understand these settings, even if they offer limited protection. For example, Facebook allows users to control data visibility, but many struggle to use the tools effectively.

**Sharing information with third parties**

Social media privacy is a major concern, as third parties can access and misuse user data. The Facebook-Cambridge Analytica breach showed data was taken without consent (Meredith, 2018). Such access exposes users to identity theft, stalking, blackmail, and other serious privacy risks.

**Security measures**

Personal data security awareness involves understanding social media security measures to prevent cyberattacks caused by user ignorance. Users must learn basic protections—like using strong passwords, avoiding information disclosure, updating software, and using antivirus tools—to reduce third-party threats (Kurniawan, 2023; Lavany & Santharooban, 2021).

**Privacy protection behavior**

Individuals use various strategies to safeguard their online privacy, especially amid concerns over data collection and third-party disclosure. Privacy protection involves limiting shared personal information on social media (Park & Kim, 2020) and applying safeguards (Baruh et al., 2017). Protective behaviors, such as adjusting privacy settings and controlling disclosures, help users manage perceived privacy risks (Milne et al., 2009). User behavior plays a vital role in privacy management by enabling selective sharing of information and interests within social networks. These actions reflect a proactive approach to protecting personal data in today's digital environment.

For this study, we considered the following indicators to be routinely performed: limiting search engines, controlling followers, reviewing posts, limiting contact, blocking users, limiting connections, disabling location services, receiving notifications, and utilizing 2-Step verification.

**Perceived privacy risk and privacy protection behavior**

Perceived privacy risk influences social media privacy and security behaviors, though findings are mixed. Koochaksaraee (2019) found no link between risk perception and behavior, highlighting the role of trust and privacy concerns. In contrast, Van Schaik et al. (2017) and Zhou and Liu (2017) found that higher perceived risks lead to more precautionary actions and privacy protections, especially among Facebook users and Chinese teenagers.

The given hypothesis was tested based on the given scenarios. (H1): There is no significant relationship between perceived privacy risk and the privacy behavior of active social media users.

**Privacy awareness and privacy protection behavior**

Studies have shown a link between perceived privacy awareness and behavior. Zwilling et al. (2022) found a positive relationship between cybersecurity awareness and protection behaviors. As awareness increased, so did efforts to prevent cyberattacks. Those with greater cybersecurity knowledge took more precautions, especially when using familiar defense methods. Additionally, individuals' understanding of internet use influenced how awareness translated into protective actions, suggesting that digital literacy plays a key role in shaping effective privacy behaviors.

Given the scenario, the following hypothesis was examined: (H2): There is no significant relationship between awareness and the behavior of active social media users.

**Synthesis of the Literature**

We looked at how privacy risks and how aware people are of privacy affect their behavior online. Most studies say that when people think there's more risk and are more aware, they are more likely to act safely on social media. But most of this research focuses on general groups of people, not specifically on students at private colleges, who might have different challenges and ways of using the internet. Also, many studies look at risk and awareness separately, not together, when it comes to how they affect privacy actions. This study aims to fill those gaps by looking at these factors within a private college setting. The goal is to create a real-world program that helps students better protect their privacy online through education and training.

**Conceptual framework**

The conceptual model shows how privacy risk, privacy awareness, and privacy protection behavior are connected among social media users at a private college. The focus of the study is on the students, who serve as the primary subjects of the research. The two main factors are looked at: privacy risk and privacy awareness. Privacy risk means how much people think they are in danger from using social media, like having their identity stolen, their data leaked, or their personal info used wrongly. Privacy awareness is about how much people know and understand privacy issues and the ways they can keep their personal data safe. Both factors are thought to affect privacy protection behavior, which is what people do to keep their privacy safe online.

Specifically, Hypothesis 1 (H1) assumes that individuals who perceive greater risks are more likely to engage in protective behaviors, while Hypothesis 2 (H2) assumes that individuals with higher levels of awareness will also demonstrate stronger privacy protection behaviors. The model also shows how this study can help in real life. The connections between these factors will be used to create a social media education and training program. This program is meant to help students learn more about privacy and how to protect themselves online. In short, the conceptual model gives both a theory and a practical way to link how people see risks and awareness to their actions, and how that can lead to better ways of using social media safely and responsibly.

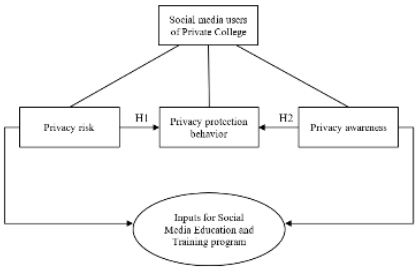


**Figure 1. Proposed conceptual model**

## METHODS

**Research Design**

The present study employed a quantitative and descriptive correlational research method to assess if perceived privacy risk and awareness influence privacy behavior in the use of social media. Quantitative research involves collecting, analyzing, and interpreting narrative and non-numerical data to

understand better a given situation (Gay et al., 2006). This study was classified as descriptive research that aims to provide a detailed account of a phenomenon and its attributes. Descriptive correlational research is employed to depict the relationship between variables rather than to deduce causal relationships. (Lappe, 2000).

**Subjects**

The sample selection employed a stratified random sampling technique, employing college departments as the stratum to ensure proportional allocation. Stratified sampling is a random sampling technique in which researchers divide a population into smaller sections based on comparable characteristics and then randomly choose a sample from these groupings (Simkus, 2022). The sample came from Colegio de San Juan de Letran (CSJL) in Manila. The population sample consisted of 332 collegiate students who were enrolled at CSJL during the second semester of SY 2022-2023. More than 98% of college-aged individuals use SMPs. (Zedd, 2023).

**Study site**

The study focused on collegiate students at CSJL in Intramuros, Manila. The sample consists exclusively of collegiate students who have active social media accounts. School is ideal for the study because college students who grew up with social media need validation and affirmation more than ever (Zedd, 2023).

**Instrumentation**

The questionnaire was adapted from previous research conducted in privacy studies. The items concerning perceived risks and behaviors were adapted from Koochaksaraee (2019), while those about privacy awareness came from Tuunainen et al. (2009). The questionnaire was divided into five sections to gather the needed information from participants. Part 1 of the study includes the students' profiles, social media use, and frequency of use. Part 3 focused on their perception of the risks associated with SMPs. Part 4 covers awareness of security and privacy, while the final part refers to behavior on social media.

A pilot test at another school assessed the survey's reliability using Cronbach's alpha, which measured internal consistency (Tavakol & Dennick, 2011). The resulting value of 0.924 indicates strong reliability, confirming that all test items used in the survey instrument are acceptable for this research.

**Data collection procedure and ethical consideration**

After determining the scope of the study, we implemented a systematic protocol to begin data collection. Permission to collect responses from higher education departments was asked by the Research and Publications Department. The RPD endorsement letter was then sent to the respective department, informing them of the matter. The survey was conducted in person (pen and paper).

The research followed ethical standards, ensuring students' voluntary participation and compliance with the Data Privacy Act of 2012. Informed consent was obtained through the survey's first page, which outlined research details and participant rights. Selecting "yes" indicated consent. Confidentiality was maintained by avoiding the use of identifiable personal information.

**Data analysis**

The data were collected, processed, and analyzed using various statistical methods. The percentage of data in the profile (gender, age, department, and year level) was calculated using frequency and percentage distribution. Then, weighted mean was used to calculate the average response value for privacy perception, awareness, and protection behavior.

The Pearson correlation coefficient was used to assess the relationship between the variables in the study, which include privacy perception, awareness, and protection behavior. Finally, data were evaluated using SPSS software with a significance level of 0.05.

# RESULTS

## Demographic Profile

**Table 1. Profile of Respondents**

| Demographic Profile | | Frequency | Percentage |
|---|---|---|---|
| Sex | Male | 132 | 39.8 |
| | Female | 200 | 60.2 |
| Age | 17-19 years old | 113 | 34.0 |
| | 20-22 years old | 196 | 59.0 |
| | 23 and above | 23 | 6.9 |
| Department | CBAA | 183 | 55.1 |
| | CLAS | 89 | 26.8 |
| | CEIT | 55 | 16.6 |
| | COED | 5 | 1.2 |
| Year Level | Freshmen | 104 | 31.3 |
| | Sophomore | 147 | 44.3 |
| | Junior | 50 | 15.1 |
| | Senior | 30 | 9.0 |
| **TOTAL** | | **332** | **100** |

The table indicates that out of 332 participants, 60.2% (f = 200) are female, and 39.8% (f = 132) are male. The table shows that 59% of respondents are 20–22 years old, and 34% are 17–19 years old. The remaining 6.9% are 23 years old or older. In addition, most of the respondents (55.1%) were from CBAA, followed by 34% from CLAS, 16.6% from CEIT, and only 5% from COED. Regarding the academic year level, 147 students are sophomores (44.3%), 104 are freshmen (31.3%), 50 are juniors (15.1%), and 30 are seniors (9%).

**Social Media Platforms and their frequency of use**

Figure 2 depicts the SMPs used by respondents and their frequency of use.

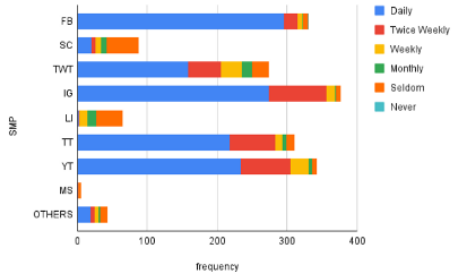


**Figure 2. Frequency of use of social media platforms**

The table reveals that 99.7% of the 332 people use Facebook, while Instagram was the second most popular SMP among the 332 respondents, with 311 (93.7%) individuals using it. YouTube was ranked third by 93.1% of respondents. Other SMPs include TikTok (79.25%), Twitter (46.15%), and Snapchat (13.6%). Most respondents utilize the top three SMPs daily, as the graph illustrates. Some respondents used these platforms on a biweekly or weekly basis.

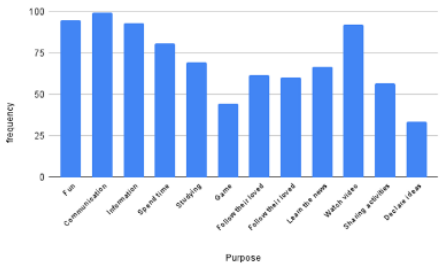


**Figure 3. Purpose of social media use**

Figure 3 shows that most respondents (99%) use SMP for communication purposes, followed by enjoyment (95%), information (93%), and watching movies (92%).

**Perceived privacy risk**

Table 3 displays the perceived risks of utilizing SMPs.

**Table 3. Perceived Risks Involved in Using Social Media Platforms**

| Statements | Mean | Interpretation |
|---|---|---|
| 1. The risk of social media security threats to the average user. | 3.91 | Very High |
| 2. The risk of social media privacy breaches to an average user. | 3.96 | Very High |
| 3. The chance that an average user will fall victim to a security breach through social media. | 3.93 | Very High |
| 4. A social media users' vulnerability to security and privacy issues. | 4.06 | Very High |
| **Weighted Mean** | **3.95** | **Very High** |

Respondents perceived social media usage as very high risk (mean = 3.95). It is vulnerable to security and privacy issues (mean = 4.06). Additionally, respondents believed that average users were at a very high risk of having their social media privacy violated (mean = 3.96). Furthermore, the chance that an average user will fall victim to a security breach (mean = 3.93) or security threat (mean = 3.91) is also very high.

**Privacy awareness**

Table 4 presents the respondents' level of awareness regarding the security and privacy features of the social media platforms (SMPs) they use.

**Table 4. Awareness of Security and Privacy**

| Statements | Mean | Interpretation |
|---|---|---|
| 1. Visibility of profile information.. | 4.40 | Extremely Aware |
| 2. Privacy Setting | 4.28 | Extremely Aware |
| 3. Sharing Information with Third Party | 4.48 | Extremely Aware |
| 4. Security Measures | 3.87 | Very Aware |
| **Weighted Mean** | **4.15** | **Very Aware** |

Table 4 indicates that the respondents possess a high level of awareness regarding the security and privacy of the various SMPs they utilize, with an overall mean score of 4.15. Respondents are "extremely aware" that they may share information with a third party (mean = 4.48), their profile information is visible (4.40), and they have knowledge of privacy settings (mean = 4.28). However, they are "very aware" of the security measures to protect their account (mean = 3.87).

**Privacy protection behavior**

Table 5 presents the respondents' frequency of engaging in various privacy protection behaviors on social media to ensure the security of their accounts.

**Table 5. Privacy Protection on Social Media**

| Indicators | Mean | Interpretation |
|---|---|---|
| 1. Limit search engines | 4.02 | Often |
| 2. Control followers | 4.24 | Always |
| 3. Review posts | 4.61 | Always |
| 4. Restrict contact | 4.30 | Always |
| 5. Block users | 3.69 | Often |
| 6. Limit connections | 4.37 | Always |
| 7. Disable location services | 4.27 | Always |
| 8. Get notifications | 4.64 | Always |
| 9. Use 2-Step verification | 4.52 | Always |
| **Weighted Mean** | **4.29** | **Always** |

Table 5 displays social media users' various privacy protection behaviors to safeguard their accounts. Respondents "always" receive notifications when their accounts are accessed from new devices (mean = 4.64) and review posts or photos in which they are tagged (mean = 4.61). Moreover, they "always" use 2-step verification (mean = 4.52), limit connections (mean = 4.37), disable location services (mean = 4.27), and control followers (mean = 4.24). On the other hand, respondents "often" limit search engines and block users, if necessary, especially those with malicious intent (mean = 3.69).

**Relationship between perceived risk and awareness with protective behavior**

Table 6 shows the Pearson-R correlation coefficient outcomes for the relationship among perceived risks, privacy awareness, and behavior on social media

**Table 6. Relationships of Perceived Risks and Awareness to Privacy Protection Behavior on Social Media**

| Variables | | Pearson-*r* | *p-value* | Decision | Conclusion |
|---|---|---|---|---|---|
| Risks | Behavior | .163 | .003 | Reject Ho | Significant |
| Awareness | | .339 | .000 | Reject Ho | Significant |

The table shows a weak positive correlation (r =.163) between perceived risks and behavior. A moderately positive correlation (r =.339) exists between awareness and behavior. The hypotheses are both rejected since their p-values are.003 and.000, respectively.

## DISCUSSION

**Demographic Profile**

The study shows that most participants are female sophomores aged 20–22 from CBAA. Meltwater (Howe, 2023], 2022) reported that 53.5% of social media users in the Philippines are female. Compared to men, women are more vocal, expressive, and open. The SMP helps them make new friends and stay in touch with family and friends.

**Social Media Platforms and their frequency of use**

Social media is increasingly ingrained in people's lives. The study's findings indicate that Facebook, Instagram, and YouTube are the most frequently utilized SMPs among the participants. These findings corresponded to the data provided by Statista and the previous study conducted by Wang et al. (2019). Most respondents cited the top four reasons for using social media: communication, entertainment, information, and watching videos. Similar results were found in the study of Torrijos-Fincias et al. (2021), wherein entertainment and communication with peers were cited as the two primary purposes. This result also supports Oducado's (2019) claim that these SMPs enable individuals to freely explore their environment, share personal experiences, and break down communication barriers.

**Perceived privacy risk**

The findings indicate that participants exhibited high awareness of potential privacy violations on social media. It demonstrates that students are aware of potential security and privacy risks. The results indicate that participants viewed social media as a potential threat and displayed a heightened awareness of security breaches and risks associated with using SMPs. Users' general awareness of privacy risks, prior experience with privacy violations, handling highly confidential information, and personal experiences with privacy threats all impact how they perceive risk. (Gerber et al., 2018). Interestingly, Torrijos-Fincias et al. (2021) observed a correlation between security threat awareness and risk perception. Understanding privacy issues may help users recognize privacy concerns and reduce risk. It suggests that users have knowledge of the privacy dangers but are unwilling to stop using SMPs and are prepared to face the implications.

**Privacy awareness**

Generation Z exhibits a heightened awareness regarding the proper and improper utilization of their SMPs, such as Facebook, YouTube, and Instagram. The study's findings indicate that participants possess a high level of awareness regarding the potential risks of sharing personal information with third parties, the need to make their accounts private, and, to some extent, limiting it to specific followers. It demonstrates that respondents are extremely aware of the need to optimize the privacy settings of their social media accounts to safeguard their personal information. Moreover, respondents are also extremely aware of the visibility of their profile information, which allows the user to control profile visibility to selected individuals such as acquaintances or colleagues (Bartsch & Dienlin, 2016; Quinn &Epstein, 2018).

**Privacy protection behavior**

Findings revealed the respondents' different actions to safeguard the information they share on social networks. The results of this study support the claim of Baruh (2017), wherein individuals must only disclose personal information and implement privacy protection controls.

The respondents always apply these privacy protection controls: they always get notifications to ensure that they know activities going on to their accounts, review their posts to avoid bashing or negative comments, they use two-step verification to make sure that no one else is using their account for any malicious content, limit connections to avoid threats from a third party, restrict contacts by declining requests from those who are not seemingly trustworthy; they turn off location services for them not to disclose their whereabouts at a given moment; and they control followers only to those who can be trusted. However, respondents often restrict search engines to protect their privacy and only block individuals when necessary. The research of Torrijos-Fincias et al. (2021) revealed that participants employed various strategies to mitigate perceived risks on social media. These strategies include exercising sound judgment, making educated choices about the content they post, and preventing individuals suspected of having fake profiles.

**Relationship between perceived risk, privacy awareness, and protective behavior**

The research indicates a significant correlation between risk perception and privacy protection behavior. The results are consistent with Van Schaik's (2017) and Zhou and Liu's (2023) research, which found a significant correlation between social media risk perception and privacy behavior. Both studies concluded that high-risk perception leads individuals to view the online gathering, utilization, and dissemination of personal information as a significant threat to their risk, subsequently engaging in preventative measures to mitigate such risks. In line with this interpretation, individuals with frequent usage and greater exposure to SMPs tend to perceive higher levels of risk. This may be attributed to their previous experiences with specific dangers, or their enhanced perception of the risks based on their experience and knowledge gained. Generation Z reaped the benefits of social media while still preventing risks, which helped them develop strong privacy practices.

This finding contradicts Koochaksaraee (2019), who found no link between risk perception and privacy behavior. Users often accept high risks due to the perceived benefits of social media (Acquisti & Gross, 2006). Van der Schyff et al. (2023) noted that trust increases users' willingness to share information.

Furthermore, this study reveals a significant relationship between privacy awareness and privacy protection behavior. This finding is consistent with Zwilling et al.'s (2022) study, which demonstrated that awareness mediates the relationship between knowledge and behavior concerning using SMPs. The findings indicate that increased awareness of privacy on social media is associated with an increased likelihood of individuals engaging in protective behaviors against privacy threats and security breaches. Increased awareness can prompt users to protect their security and privacy in response to potential threats. Even though respondents have a strong understanding of privacy protection, ongoing education may be required to increase their awareness of privacy breaches, security threats, and security measures, which have the lowest mean among the indicators. Additionally, they need to understand the significance of limiting search engines and blocking someone from SMP to remain cautious about their privacy.

## CONCLUSION

**Theoretical contributions**

This current study attempts to fill in the gaps and, in doing so, make significant contributions. According to our search of databases that have been peer-reviewed, no previous study has empirically examined the students' risk perception and privacy awareness relationship with their privacy protection behavior in an academic setting. Furthermore, existing research on social media privacy has generally focused on integrating only one or two of the criteria stated. Several studies have also examined the link between these characteristics and privacy attitudes. Furthermore, existing research on privacy in social media use has primarily focused on specific factors such as privacy concerns, disclosure, and privacy settings.

The study's theoretical lenses are TRMU, U&G, and PMT to explain social media privacy. Although not directly tested in this study, the TRMU and U&GT are relevant as a backdrop and a framework for exploring and describing the results. The TRMU is a compelling theory about how social media has become a ritual in the lives of these students, leading to a lack of concern for privacy and personal risk. The findings show that students are very aware of the dangers of social media and have taken steps to reduce the risks and prevent adverse effects. The U&GT examines the use of social media to satisfy varying individual needs. Students see social media to unwind, have fun, meet people, and make new friends.

The research shows that SMP's gathering, utilizing, and sharing of information are perceived as a substantial risk to individuals' privacy and security. Perceived risk is positively related to protective behavior. According to the PMT, individuals are more inclined to engage in measures to safeguard their online privacy if they perceive the threat to be more significant.

**Practical implications**

Social media continues to become more significant in both daily life and education. The study has practical implications regarding the significance and nature of privacy when using SMP. Students have demonstrated a high awareness of the potential risks associated with social media usage; however, they must take the necessary precautions to mitigate these risks and prevent any adverse effects from active participation.

The institution may contribute significantly to students' privacy awareness by developing a social media education and training program to teach the students to protect their privacy. This program may include topics on the myth of total anonymity in social media, the Data Privacy Act of 2012, types of privacy threats and security breaches such as social engineering and phishing, confidentiality and social media privacy settings, and best practices for safe social networking.

Furthermore, the institution can organize a privacy day featuring speakers on data protection topics, conduct email campaigns with privacy tips, and advertise on traditional platforms like school papers and television to tackle diverse social media privacy threats.

**Limitations and Recommendations**

Although the results are noteworthy, this study has some limitations. This study only looked at Generation Z, which is more adept with technology and social media. Other demographics, such as baby boomers and Generation X, should be considered in future studies. This generation is not entirely exposed to technology and may need to familiarize themselves with the inner workings of SMPs.

We searched peer-reviewed databases and found that most research is based on a single SMP or SMPs in general. Future research may examine each SMP's privacy protection controls by comparing them. This comparison will provide possible sources for privacy education and privacy management.

The current study addresses perceived risk, privacy awareness, and protection behavior. Hence, employing a comprehensive research approach that involves other important variables is recommended. The impact of privacy on using SMP can vary depending on several factors, including benefits, privacy concerns, privacy self-efficacy, trust, beliefs, technology for protecting privacy, and privacy sensitivity.

## REFERENCES


Adams, S. (1975). Evaluative research in corrections: A Practical Guide. U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice. https://books.google.com.ph/books?id=wKq3tBspNQ4C

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: Danezis, G., Golle, P. (eds) *Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, 4258*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11957454_3

Alguliyev, R., Aliguliyev, R., & Yusifov, F. (2018). Role of social networks in e-government: risks and security threats. *Online Journal of Communication and Media Technologies, 8*(4), 363–376. https://doi.org/10.12973/ojcmt/3957

Alhabash, S., & Ma, M. (2017). A tale of four platforms: Motivations and uses of Facebook, Twitter, Instagram, and Snapchat among college students? *Social Media + Society, 3*(1). https://doi.org/10.1177/2056305117691544

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*, 26-53. https://doi.org/10.1111/jcom.12276

Bishop, M. (2019). Healthcare social media for consumer informatics. In M. Edmunds, C. Hass, & E. Holve (Eds.), *Consumer informatics and digital health: Solutions for health and health care*, 61–86. Springer Publishing. https://doi.org/10.1007/978-3-319-96906-0_4

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society, 20*, 1261-1278. https://doi.org/10.1080/1369118X.2016.1229001

Correia, J., & Compeau, D.R. (2017). Information Privacy Awareness (IPA): A review of the use, definition and measurement of IPA. *Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2017.486

Falgoust, G., Winterlind, E., Moon, P., Parker, A., Zinzow, H., & Chalil Madathil, K. (2022). Applying the uses and gratifications theory to identify motivational factors behind young adults' participation in viral social media challenges on TikTok. *Human Factors in Healthcare, 2*, 100014. https://doi.org/10.1016/j.hfh.2022.100014

Fiesler, C., Dye, M., Feuston, J. L., Hiruncharoenvate, C., Hutto, C. J., Morrison, S., Roshan, P. K., Pavalanathan, U., Bruckman, A. S., De Choudhury, M., & Gilbert, E. (2017). What (or who) is public? Privacy settings and social media content sharing. *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. 567–580. https://doi.org/10.1145/2998181.2998223

Gay, L. R., Mills, G. E., & Airasian, P. (2006). *Educational Research: Competencies for Analysis and Applications*. Columbus: Merrill Greenwood.

Gerber, N., Gerber, P. & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226-261. https://doi.org/10.1016/j.cose.2018.04.002.

Hill, M. & Swinhoe. D. (2022, November 8). *The 15 biggest data breaches of the 21st century*. CSO Online. Retrieved June 1, 2023, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Hossain, M.A. (2019). Effects of uses and gratifications on social media use: The Facebook case with multiple mediator analysis. *PSU Research Review, 3*(1), 16-28. https://doi.org/10.1108/PRR-07-2018-0023

Howe, H. (2022, November 14). *Social Media Statistics in the Philippines [Updated 2023]*. Meltwater. https://www.meltwater.com/en/blog/social-media-statistics-philippines

Jozani, M.M., Ayaburi, E.W., Ko, M.S., & Choo, K. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*. https://doi.org/10.1016/j.chb.2020.106260.

Katz, E., Blumler, J. G., & Gurevitch, M. (1973). Uses and gratifications research. *Public Opinion Quarterly, 37*(4), 509–523. https://doi.org/10.1086/268109

Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media, 3–4*, 1–21. sl

Kircaburun, K., Alhabash, S., Tosuntaş, Ş. B., & Griffiths, M. D. (2020). Uses and gratifications of problematic social media use among university students: A simultaneous examination of the big five of personality traits, social media platforms, and social media use motives. *International Journal of Mental Health and Addiction, 18*(3), 525–547. https://doi.org/10.1007/s11469-018-9940-6

Koochaksaraee, A.A. (2019). End-user security & privacy behaviour on social media: Exploring posture, proficiency & practice. . http://doi.org/10.20381/RUOR-23557

Kurniawan, Y., Santoso, S. I., Wibowo, R. R., Anwar, N., Bhutkar, G., & Halim, E. (2023). Analysis of higher education students' awareness in indonesia on personal data *Security in Social Media. Sustainability, 15*(4), 3814. https://doi.org/10.3390/su15043814

Lappe, J.M. (2000). Taking the mystery out of research. Descriptive correlational design. *Orthopaedic Nursing*, *19*(2), 81.

Lee, K., & Attablayo, P. (2023). Examining the impacts of privacy awareness on user's self-disclosure on social media. *ArXiv*. https://doi.org/10.48550/arXiv.2303.07927

Limecube. (2022, June 30). *7 ways to improve your visibility on social media*. https://www.limecube.co/7-ways-to-improve-your-visibility-on-social-media

Maddux, J.E. & Rogers, R. W. (1983). Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*. *19*(5): 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Masciantonio, A., & Bourguignon, D. (2023). Motivation Scale for Using Social Network Sites: Comparative Study between Facebook, Instagram, Twitter, Snapchat, and LinkedIn. *Psychologica Belgica, 63*(1), 30–43. https://doi.org/10.5334/pb.1161

Meredith, S. (2018, April 10). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

Milne, G.R., Labrecque, L.I., & Cromer, C.T. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*, 449-473. http://doi.org/J.1745-6606.2009.01148.X

Monti, A., & Wacks, R. (2019). *Protecting Personal Information: The Right to Privacy Reconsidered*. Hart Publishing.

Oducado, R. M., Sales, M., Magarzo, A. J., Panes, P. M., & Lapastora, J. T. (2019). Perceptions and attitude on using social media responsibly: Toward social media literacy in nursing education. *Belitung Nursing Journal, 5*(3), 116-122. https://doi.org/10.33546/bnj.789

Olpin, E., Hanson, C. L., & Crandall, A. (2023). Influence of Social Media Uses and Gratifications on Family Health among U.S. Parents: A Cross-Sectional Study. *International journal of environmental research and public health*, *20*(3), 1910. https://doi.org/10.3390/ijerph20031910

*Conference on Advanced Computer Science and Information Systems, ICACSIS 2018*. 271-276. https://doi.org/10.1109/ICACSIS.2018.8618220

Park, N., & Kim, Y. (2020). The Impact of Social Networks and Privacy on Electronic Word-of-Mouth in Facebook: Exploring Gender Differences. *International Journal of Communication, 14*, 24.

Quinn, K., & Epstein, D. (2018). #MyPrivacy: How Users Think About Social Media Privacy. *Proceedings of the 9th International Conference on Social Media and Society*. https://doi.org/10.1145/3217804.3217945

Schmidt, P., Gordoni, G., Ajzen, I., Beuthner, C., Davidov, E., Silber, H., Steinmetz, H., & Weiß, B. (2022). Twitter Users' Privacy Behavior: A Reasoned Action Approach. *Social Media + Society*, *8*(3). https://doi.org/10.1177/20563051221126085

Simkus, J. (2022, November 3). *Stratified Random Sampling: Definition, Method & Examples*. Simply Psychology. https://www.simplypsychology.org/stratified-random-sampling.html

Slovic, P. (2000). *The Perception of Risk* (1st ed.). Routledge. https://doi.org/10.4324/9781315661773

Statista.com .Most popular social networks worldwide as of January 2023, ranked by number of monthly active users. (2023, January).. Retrieved June 1, 2023, from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Tao, H., Bhuiyan, M.Z., Rahman, M.A., Wang, G., Wang, T., Ahmed, M.M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems, 98*, 660-671. https://doi.org/10.1016/j.future.2019.03.042

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education, 2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Tips for using privacy settings - Office of the Privacy Commissioner of Canada. (2019, March). *Tips for Using Privacy Settings - Office of the Privacy Commissioner of Canada*. Retrieved May 2, 2023, from https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/gd_ps_201903/?WT.ac=set-en-1

Torrijos-Fincias, P., Serrate-González, S., Martín-Lucas, J., & Muñoz-Rodríguez, J. M. (2021). Perception of risk in the use of technologies and social media. Implications for identity building during adolescence. *Education Sciences*, *11*(9), 523. https://doi.org/10.3390/educsci11090523

Tuunainen V. K., Pitkanen, O. and Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking Sites —Case Facebook. *BLED 2009 Proceedings*. 42. https://aisel.aisnet.org/bled2009/42

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 and Security*, *126*, [103071]. https://doi.org/10.1016/j.cose.2022.103071

Wang, L., Sun, Z., Dai, X., Zhang, Y. and Hu, H.-h. (2019), Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People, 32*(6), 679-1703. https://doi.org/10.1108/ITP-01-2018-0020

Zedd, E. Z. (2023, February 9). *Opinion | Social media has turned college students into mass consumers*. The Breeze. Retrieved June 2, 2023, from https://www.breezejmu.org/opinion/opinion-social-media-has-turned-college-students-into-mass-consumers/article_65ac8052-a7d9-11ed-9930-272f82cad2b1.html

Zhou, S., & Liu, Y. (2023). Effects of Perceived Privacy Risk and Disclosure Benefits on the Online Privacy Protection Behaviors among Chinese Teens. *Sustainability, 15*(2), 1657. https://doi.org/10.3390/su15021657

Zwilling, M., Klien, G.H., Lesjak, D., Wiechetek, L., Çetin, F.H., & Basim, H.N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*, 82 - 97. https://doi.org/10.1080/08874417.2020.1712269