INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH
2025, Vol. 6, No. 10, 4952 – 4962
http://dx.doi.org/10.11594/ijmaber.06.10.08

Research Article

Assessing Data Privacy Attitudes of Information Technology Students: Basis for Awareness Enhancement

Aaron Paul M. Dela Rosa*

College of Information and Communications Technology, Bulacan State University, Bulacan 3000, Philippines

Article history:
Submission 27 July 2025
Revised 30 September 2025
Accepted 23 October 2025

**Corresponding author:*
E-mail:
aaronpaul.delarosa@bulsu.edu.ph

ABSTRACT

In today's digital society, the widespread use of social media and online platforms has intensified concerns about the protection of personal information. This study examined the data privacy attitudes of Information Technology (IT) students at Bulacan State University, who are among the most engaged users of digital technologies. Using a descriptive survey administered to 350 students across year levels, the study explored their awareness of privacy policies, attitudes toward data sharing, and comfort with online tracking. Results indicated that while most students expressed high concern for online privacy and rated it as highly important, many simultaneously valued the benefits of free access to social media platforms despite potential risks to their personal information, demonstrating the persistence of the privacy paradox. Students also showed discomfort with being tracked for targeted advertising, yet their reliance on Facebook and other platforms underscores vulnerabilities in privacy practices. A majority recommended that privacy awareness training be provided during their first year of study, highlighting the need for early intervention. Findings suggest that embedding privacy literacy in the IT curriculum, institutionalizing university-wide orientations, and aligning with the Philippine Data Privacy Act of 2012 are essential to building a culture of responsible data handling and compliance in higher education.

Keywords: *Data Privacy, Data Privacy Awareness, Information Technology, Online Privacy, Privacy Attitudes*

Background

Nowadays, almost everyone is using the internet to share their information on different available platforms. In this advancing digital age of big data and artificial intelligence, individuals should be more careful about how they share their information, specifically sensitive personal information, online (Wachter & Mittelstadt, 2019). Additionally, individuals should be more aware of how their data is

How to cite:
Dela Rosa, A. P. M. (2025). Assessing Data Privacy Attitudes of Information Technology Students: Basis for Awareness Enhancement. *International Journal of Multidisciplinary: Applied Business and Education Research*. *6*(10), 4952 – 4962. doi: 10.11594/ijmaber.06.10.08

being processed by different online platforms and whether it adheres to the General Data Protection Regulation (GDPR). GDPR provides principles, provisions, standards, and guidelines for different countries to follow in implementing data privacy (General Data Protection Regulation [GDPR], 2022).

The Republic of the Philippines is one of the many countries implementing its data privacy law patterned after GDPR. The Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA), provides policies, standards, and guidelines on how data privacy in the Philippines should be handled by companies, institutions, and even universities (National Privacy Commission [NPC], 2012). Everything a Filipino must know regarding data privacy, its provisions, the National Privacy Commission (NPC), processing of personal information, rights of the data subject, security of personal information, accountability for transfer of personal information, security of sensitive personal information in government, and penalties is all provided within the DPA. According to the study conducted by NPC in 2017, 94% of Filipinos cared about how their personal data is being processed, while 85% agreed that their rights as data subjects are important (NPC, 2017). Additionally, in the University of the Philippines forum roundtable discussion in 2019, their medical records division is aware of the DPA and implements measures to ensure that their data are protected (University of the Philippines [UP], 2019).

Bulacan State University (BulSU) is one of the state universities situated in the City of Malolos, Bulacan, that implements data privacy. BulSU provides a privacy policy to its students that serves as a guide on how the students' data is processed. Additionally, students' rights as data subjects are provided for them to be aware of what their rights are according to the DPA (Bulacan State University [BulSU], 2022). Since data privacy deals with personal information being processed in information and communications systems, students should be aware of how their information is being collected and processed since their admission to the university. Information Technology (IT) students, being more aligned with such a concern, specifically in this digital era, should be more aware of such policies of the university and the DPA (Bhatnagar & Pry, 2020), and should have better attitudes toward sharing personal information on different online platforms they are using for personal and educational purposes (Kokolakis, 2017; Namara et al., 2018).

This study aims to determine the data privacy attitudes of the students of BulSU, specifically IT students, in DPA, and how they are performing online, since these students are more involved in this digital era. Additionally, this study aims to provide a basis for awareness of DPA and its implementing rules and regulations to the students at the university.

This study answered the following research questions explicitly: (1) What is the most common social media platform for sharing personal information? (2) How can students' data privacy attitudes on using social media platforms be assessed? And (3) When should training on data privacy awareness be offered to students?

Related Work

Online Data Privacy Attitudes

The rapid growth of social media platforms has intensified debates over how personal data is collected, shared, and monetized. Research consistently shows a gap between expressed privacy concerns and actual online behaviors, a phenomenon widely referred to as the privacy paradox (Barth & de Jong, 2017; Kokolakis, 2017). More recent studies confirm this paradox among university students, who claim to value privacy yet continue to disclose personal information in exchange for convenience or free access (Kaya & Yaman, 2022; Connolly et al., 2025). Studies on student populations further reveal that while many are aware of privacy policies, their actual practices remain inconsistent, leaving them vulnerable to targeted advertising and misuse of personal data (Ayop et al., 2025; Baldwin et al., 2023).

This paradox is especially evident in higher education contexts, where students' frequent reliance on platforms such as Facebook, Instagram, and TikTok exposes them to privacy risks despite their stated concerns (Barth & de Jong, 2017; Kaya & Yaman, 2022). Understanding these contradictory behaviors is crucial to designing effective privacy awareness programs tailored to youth and student populations.

The Privacy Paradox

A consistent theme in privacy research is the contradiction between individuals' stated concerns about protecting their personal data and their actual behaviors online, a phenomenon widely known as the privacy paradox (Barth & de Jong, 2017; Kokolakis, 2017). University students, in particular, often report that privacy is highly important to them, yet willingly disclose sensitive information on social media platforms in exchange for social connectivity, entertainment, or free access (Connolly et al., 2025). This paradox suggests that students may cognitively recognize the risks of data misuse but behaviorally prioritize the immediate benefits of digital participation, reflecting a gap between awareness and practice.

Recent studies have highlighted how this paradox manifests among youth and student populations. For example, Kaya and Yaman (2022) found that while most students expressed concern over personal data collection, their disclosure patterns remained largely unchanged when faced with privacy warnings. Similarly, Baldwin et al. (2023) observed that although students valued privacy, they lacked the necessary knowledge to effectively manage social media settings, leaving them exposed to profiling and targeted advertising. In the Philippine context, where Facebook penetration rates are among the highest globally, the paradox is especially critical: students' reliance on social media platforms makes them vulnerable, even as they express discomfort with surveillance and targeted ads. Understanding this paradox is essential for universities, as it highlights the need for interventions that go beyond awareness-raising to actively change behaviors through education, policy, and compliance with the Data Privacy Act of 2012.

Data Privacy Awareness

Awareness of privacy rights and risks is a critical determinant of protective behaviors online. Education, institutional policies, and media literacy significantly influence how students understand and manage their digital identities (Bartsch & Dienlin, 2016; Wissinger, 2017). However, studies highlight persistent awareness gaps among university students, particularly in developing countries, where privacy literacy programs are often underdeveloped (Baldwin et al., 2023; Connolly et al., 2025). In the Philippines, the National Privacy Commission (NPC, 2017) reported that while 94% of Filipinos expressed concern over how their personal data was processed, only a minority could articulate their legal rights under the Data Privacy Act of 2012. Recent local discussions, such as the University of the Philippines' 2019 forum on data privacy practices, reveal both progress and ongoing challenges in compliance at the institutional level.

These findings underscore the need to embed structured privacy awareness initiatives within higher education. By addressing gaps in student knowledge early, through curriculum integration, orientations, and compliance-based training, universities can reduce risks and strengthen adherence to national data protection laws.

Methods

Research Design

This study employed a descriptive survey design to capture the data privacy attitudes of Information Technology (IT) students. Descriptive surveys are useful for systematically gathering opinions, perceptions, and attitudes from a target population at a given point in time (Fraenkel et al., 2019).

Research Instrument

The survey instrument was adapted from Bhatnagar and Pry (2020), which originally assessed students' perceptions of privacy and cybersecurity. For this study, only the data privacy–related questions were retained, resulting in 11 items covering privacy attitudes, awareness, and perceptions. Responses included both dichotomous (Yes/No) and Likert-scale items.

It should be noted that the instrument was not pilot-tested, and no internal consistency measure (e.g., Cronbach's alpha) was calculated. While this limits the ability to establish reliability and validity statistically, the instrument was grounded in prior research and adapted to the Philippine context for relevance.

Data Gathering Procedure

The survey was administered online via a Google Form to maximize accessibility and participation. Faculty members shared the form with their classes, and student organizations helped circulate the link. In some instances, researchers visited classes directly to encourage participation. Respondents were assured of the confidentiality of their responses and the voluntary nature of their participation.

Population and Sample

The target population consisted of approximately 2,500 Bachelor of Science in Information Technology (BSIT) students enrolled at Bulacan State University across four year levels. A minimum sample size of 333 was determined using Slovin's formula at a 5% margin of error.

Although the study initially intended random sampling, in practice, data were collected using convenience sampling. The online survey form was disseminated through faculty coordinators, student organizations, and direct distribution in classrooms. A total of 350 responses were collected, slightly exceeding the required sample size.

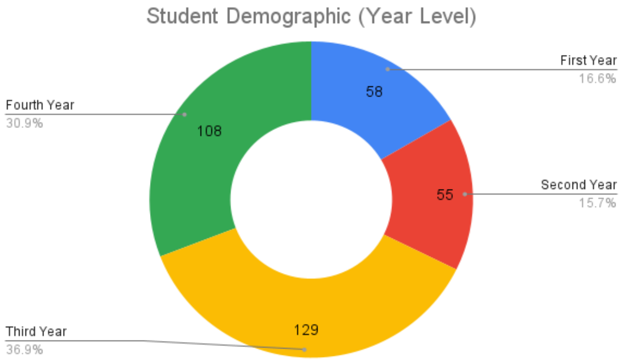

Figure 1. Student demographics that present the year-level distribution of the BSIT students

Statistical Treatment

To analyze the student responses, this study utilized mean, frequency distribution, and percentage computation. Most of the questions are answerable with yes or no. On one of the questions, students were asked to answer a five-point Likert scale where five (5) has a descriptive interpretation of "Very Important" and one (1) has "Unimportant." The question is about how important privacy is to the students.

Limitations

This study is subject to several limitations that should be considered when interpreting the findings. First, the survey instrument, although adapted from prior research, was neither pilot-tested nor evaluated for internal consistency using Cronbach's alpha. As such, the reliability of the measures cannot be statistically assured. Second, the use of convenience sampling rather than true random sampling introduces potential bias, as participation depended on students' willingness to respond, which may limit the representativeness of the sample. Third, the reliance on self-reported data raises the possibility of social desirability bias, with students perhaps overstating their concern for privacy or underreporting risky behaviors. Fourth, the study was conducted within a single university, which restricts the generalizability of results to other higher education institutions in the Philippines. Lastly, given the descriptive nature of the design, the study identifies patterns and associations but cannot establish causal relationships. Despite these limitations, the findings provide valuable insights into the privacy attitudes of IT students and highlight the importance of strengthening awareness and institutional policies on data protection.

Result and Discussion

Social Media Used by IT Students

To understand the students' data privacy attitudes online, they were asked if they were using any social media. 100% (350 out of 350) of the students answered that they are using social media. Figure 2 presents the different social media used by the students, and Figure 3 shows their social media status.

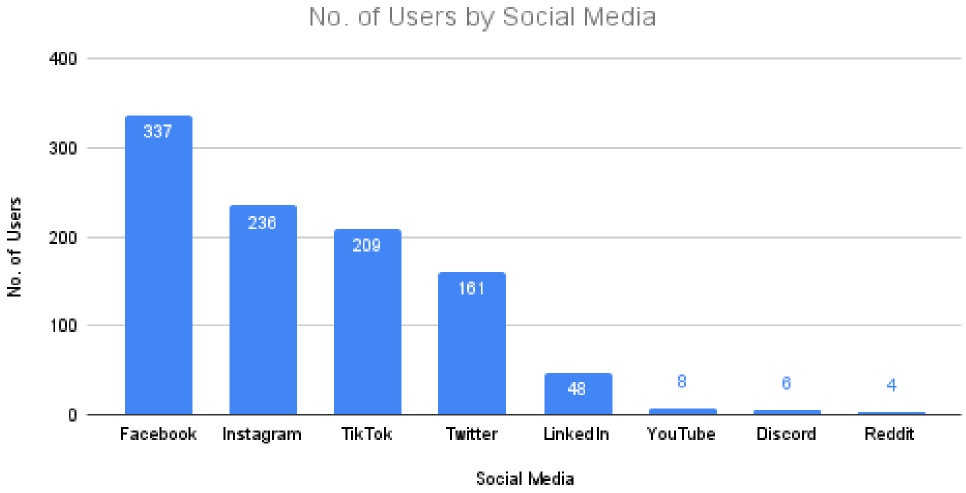

Figure 2. Different social networking sites used by the students and their corresponding frequency of users

Facebook was the dominant platform among respondents (96.3%), followed by Instagram (67.4%) and TikTok (59.7%). This strong preference mirrors national trends in the Philippines, where Facebook is the most widely used social media service. However, reliance on a single dominant platform increases vulnerability to data privacy risks, as past scandals involving Facebook highlight how user data can be exploited for advertising or political purposes (Kaya & Yaman, 2022). The fact that students reported using multiple platforms further broadens their digital footprint, reinforcing the need for privacy education that goes beyond platform-specific policies and instead cultivates a holistic understanding of online risks.

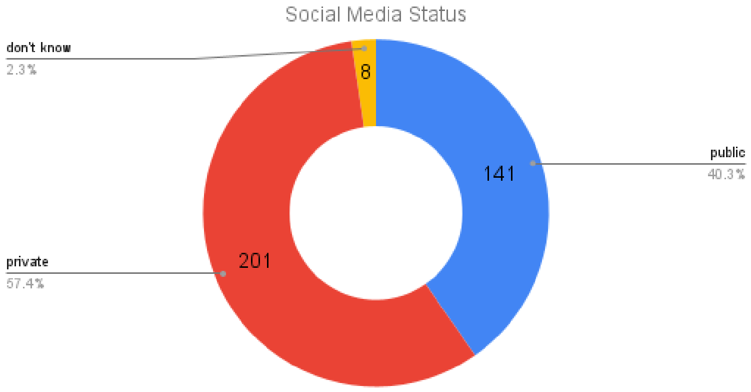

Figure 3. Social media status of the students

After determining their social media platforms, students were asked about their social media status. Over half of respondents (57.4%) kept their accounts private, while 40.3% maintained public profiles. The sizable portion of students with public accounts signals a continued willingness to expose personal data despite acknowledging risks. This behavior aligns with findings from Connolly et al. (2025), who argue that students often underestimate the consequences of public exposure until breaches occur. The presence of students who were unaware of their privacy settings (2.3%) underscores gaps in digital literacy, suggesting that many students lack the skills to navigate basic privacy configurations effectively.

Students were asked how important privacy is to them, specifically on using these different social media platforms. Figure 4 presents the students' responses using a five-point scale on how important privacy is to them.

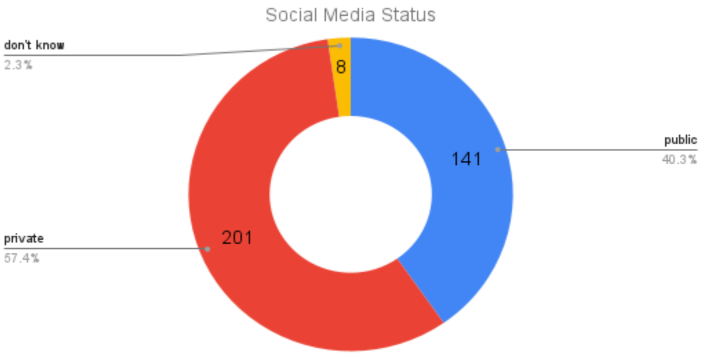

Figure 4. Importance of privacy for students

Most students rated privacy as "very important" (M = 4.78, SD = 0.471), indicating high concern for data protection. Yet, this concern does not consistently translate into protective behaviors, as subsequent figures demonstrate. This contradiction reflects the privacy paradox, where users simultaneously value privacy while engaging in practices that compromise it (Kokolakis, 2017). The high self-reported importance of privacy may also reflect social desirability bias, further highlighting the gap between what students say and what they do.

Students' Data Privacy Attitudes on Using Social Media Platforms

To determine the online privacy of the students on using social media platforms, they were asked multiple questions regarding privacy policies, how their data is being used by the providers, having a free social media application against its risk of personal information usage for big data analytics, and if they are comfortable with being tracked for targeted advertising. Figures 5-8 present the responses of the students, commonly answerable by a "yes" or a "no."

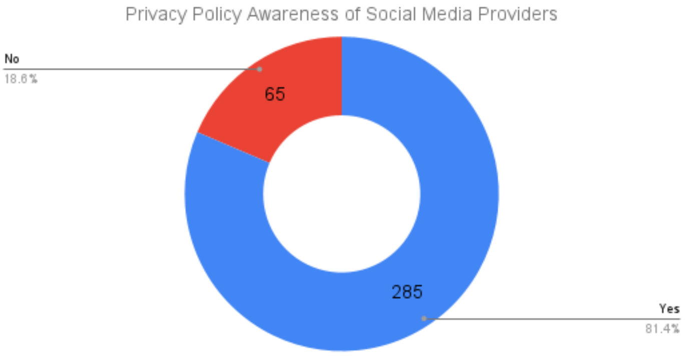

Figure 5. Students' awareness of the privacy policy of the social media providers

As seen in Figure 5, a majority of students (81.4%) reported awareness of privacy policies. While this suggests exposure to data protection information, awareness alone may not equate to understanding. Prior studies indicate that most users skip or skim privacy policies due to length and complexity (Baldwin et al., 2023). Thus, while students acknowledge the existence of policies, their ability to critically interpret and apply these terms in protecting their data remains questionable.

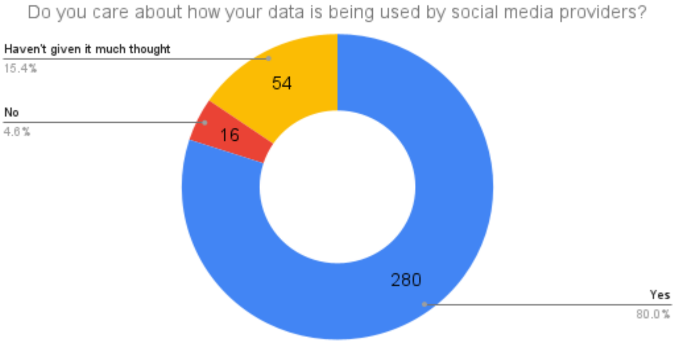

Figure 6. Students' level of care about how their data is being used by social media providers

Eighty percent of respondents expressed concern about how their data is used by providers. However, 20% admitted they had not given it much thought, indicating uneven levels of engagement with privacy issues. This suggests that concern is not uniformly distributed and may be influenced by digital literacy or prior experiences. Ayop et al. (2025) note that awareness gaps can lead to passive acceptance of data use, leaving students vulnerable to manipulation through profiling and targeted ads.

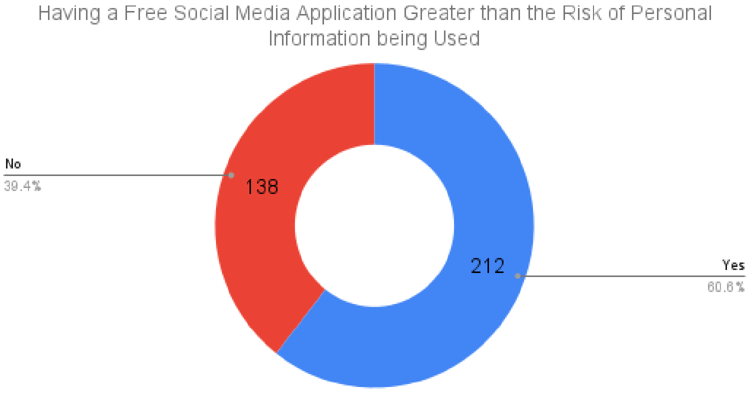

Figure 7. Student responses on the advantages of having a free social media application

Interestingly, 60.6% of students felt that the advantages of free access outweighed the risks to their personal information. This is a strong illustration of the privacy paradox: although students value privacy, they continue to prioritize convenience and accessibility over protection (Connolly et al., 2025). Such tradeoffs highlight why mere awareness campaigns are insufficient; universities must actively foster critical digital decision-making skills to help students evaluate the long-term costs of sacrificing privacy for short-term benefits.

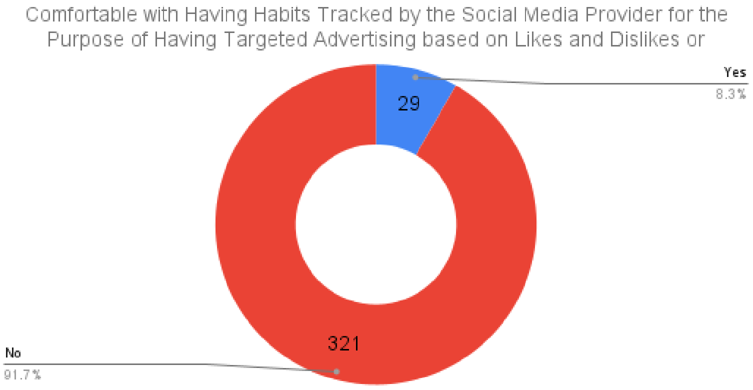

Figure 8. Student responses on being tracked by social media providers for targeted advertising

Most respondents (91.7%) expressed discomfort with being tracked for targeted advertising, contrasting with their willingness to accept free access in Figure 7. This selective resistance suggests that the framing of privacy threats matters. Students may tolerate abstract risks but reject practices like tracking when described in personal terms. These findings align with Kaya and Yaman (2022), who found that students were particularly sensitive to surveillance-related terminology. This points to an opportunity for awareness programs to use concrete examples to bridge the gap between abstract privacy concepts and lived experiences. Table 1 presents the cross-tabulation of students' year levels and privacy attitudes.

Table 1. Cross-tabulation of Year Level and Students' Privacy Attitudes

Year Level	Aware of Privacy Policies (%)	Rated Privacy "Very Important" (%)	Prefer Free Access Over Privacy Risks (%)
1st Year	58.62	79.31	62.07
2nd Year	83.64	87.27	58.18
3rd Year	88.37	74.42	62.02
4th Year	84.26	86.11	59.26

The cross-tabulation presents notable variations in privacy attitudes across year levels. Awareness of privacy policies increased sharply from first-year (58.62%) to third-year students (88.37%), suggesting that as students progress through their program, exposure to academic content and institutional guidelines enhances their familiarity with data protection principles. However, awareness slightly declined among fourth-year students (84.26%), which may indicate that privacy literacy development is uneven or that senior students become more complacent once accustomed to online practices.

The perceived importance of privacy followed a similar pattern, peaking among second-year students (87.27%) and dipping to 74.42% in the third year before rising again in the fourth year (86.11%). This fluctuation could be due to differing course exposures or shifting academic priorities as students advance. Despite these variations, the majority across all levels still rated privacy as important, reflecting consistent recognition of its relevance.

Interestingly, a substantial proportion of students across all year levels continued to prefer free access to social media despite the potential risks (ranging from 58.18% to 62.07%). This persistent tendency demonstrates the privacy paradox, the coexistence of strong privacy concerns with behaviors that undermine them (Connolly et al., 2025; Kokolakis, 2017). Even among more experienced students, convenience and accessibility appear to outweigh caution, indicating that awareness alone does not necessarily translate into privacy-conscious action.

Overall, these results underscore the importance of early and continuous privacy education. Since first-year students show lower awareness and a stronger tendency toward risky behaviors, integrating data privacy training at the entry level is essential. Reinforcing these concepts in upper-year courses could help sustain awareness and foster long-term behavioral change aligned with the objectives of the Philippine Data Privacy Act of 2012.

Students' Training on Data Privacy Awareness

As part of the survey, students were asked if there should be training on privacy awareness and when it should be offered. Figures 9-10 present the students' responses to these questions.

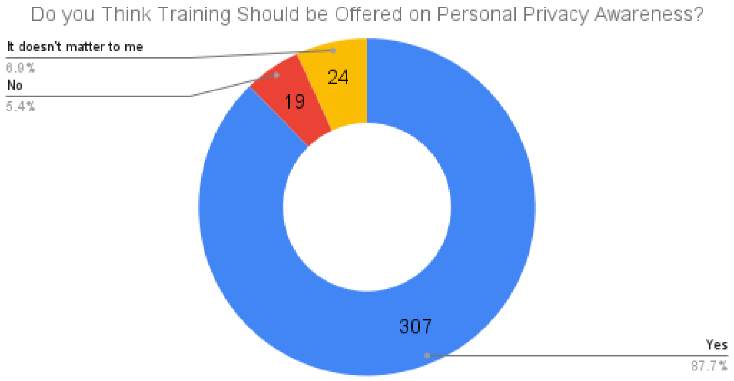

Figure 9. Student responses should there be training to be offered on privacy awareness

The majority (87.7%) agreed that training on privacy awareness should be provided, reinforcing that students recognize the importance of institutional support. However, the presence of a small group (12.3%) who indicated disinterest suggests that awareness is not universally valued. This echoes the argument of Ayop et al. (2025), who emphasize that interventions must be engaging and context-sensitive to reach students who may otherwise dismiss privacy as irrelevant.

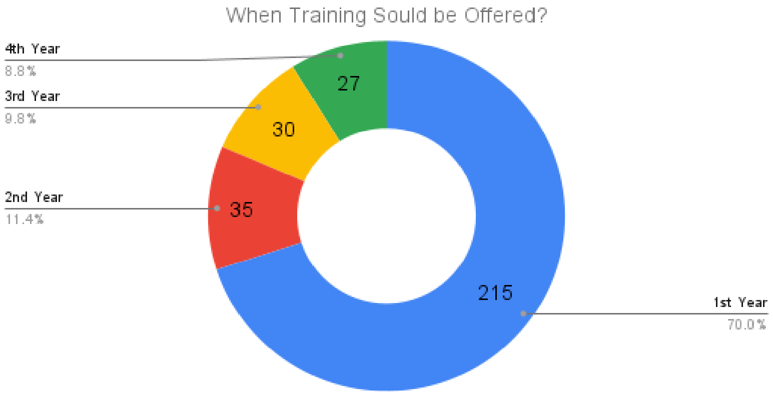

Figure 10. Student responses regarding the year level at which the training should be offered

Among those who supported training, 70% preferred it during the first year of study. This reflects an understanding that early intervention is critical, as students form their online habits early in their university experience. Implementing data privacy training at the entry level would allow institutions to establish a foundation of responsible practices that can be reinforced in higher years. Linking such training to compliance with the Data Privacy Act of 2012 would not only benefit students but also strengthen institutional accountability in the Philippine higher education sector.

Conclusion

This study highlighted that IT students recognize the importance of data privacy but often make trade-offs between convenience and protection, a clear manifestation of the privacy paradox. While most students kept accounts private and expressed discomfort with tracking, many still valued the benefits of free access to social media platforms. The findings emphasize the need for structured interventions: integrating privacy literacy into IT education, conducting university-wide orientations, and partnering with the National Privacy Commission for compliance-based programs. Embedding these measures as part of institutional policy not only equips students with the knowledge to safeguard their digital identities but also strengthens universities' adherence to the Data Privacy Act of 2012. By prioritizing awareness at the earliest stages of higher education, academic institutions can foster a culture of responsibility and resilience in the face of evolving digital privacy challenges.

Based on the findings, the following actions are recommended to strengthen student data privacy awareness and institutional compliance: (1) Embed privacy literacy and responsible digital citizenship modules in core IT courses, ensuring students gain structured and progressive training throughout their program, (2) Require mandatory privacy awareness orientations for all incoming students across disciplines, not limited to IT, to establish a baseline understanding of data protection principles, and (3) Institutionalize privacy awareness programs as part of higher education compliance measures under the Data Privacy Act, making them a standard requirement for accreditation and quality assurance.

Acknowledgement

This research does not receive any source of funding. The author would like to acknowledge the BulSU-CICT BSIT students, batch 2022-2023, for participating in this research as respondents.

References

Ayop, J. R., Larecion, R. C., Respulo, A. A. P., Villasurda, R. A. S., Arendain, K. M. A., & Cantil, J. B. J. (2025). Relationship of Social Media Usage and Data Privacy Awareness among College Students in the Municipality of Bansalan. *Asian Journal of Education and Social Studies, 51*(7), 617–627. https://doi.org/10.9734/ajess/2025/v51i72152

Baldwin, L., Gores, J., & Kilbride, J. (2023). Social media use and awareness of privacy concerns. *Concordia Journal of Communication Research, 8*, 1-21. https://doi.org/10.54416/HQWT8424

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

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Information Systems Education Journal, 18(1), 48-58. https://eric.ed.gov/?id=EJ1246231

Bulacan State University (BulSU). (2022). Data Privacy. https://bulsu.edu.ph/data-privacy/

Connolly, L. Y., Lang, M., & Giboney, J. (2025). A study of the privacy paradox amongst young adults in the United Arab Emirates. *Telematics and Informatics Reports, 19*, 100248. https://doi.org/10.1016/j.teler.2025.100248

Fraenkel, J. R., Wallen, N. E., Hyun, H. H. (2019). How to design and evaluate research in education. McGraw-Hill Education. https://saochhengpheng.files.wordpress.com/2017/03/jack_fraenkel_norman_wallen_helen_hyun-how_to_design_and_evaluate_research_in_education_8th_edition_-mcgraw-hill_humanities_social_sciences_languages2011.pdf

General Data Protection Regulation (GDPR). (2022). Complete guide to GDPR Compliance. https://gdpr.eu/

Kaya, S., & Yaman, D. (2022). Examining university students' online privacy literacy levels on social networking sites. *Participatory Educational Research, 9*(3), 22-45. http://dx.doi.org/10.17275/per.22.52.9.3

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Society, 64, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Namara, M., Sloan, H., Jaiswal, P., & Knijnenburg, B. P. (2018). The potential for user-tailored privacy on Facebook. 2018 IEEE Symposium on Privacy-Aware Computing (PAC) (pp. 31-42). IEEE. https://doi.org/10.1109/PAC.2018.00010

National Privacy Commission (NPC). (2012). Republic Act 10173 - Data Privacy Act of 2012. https://www.privacy.gov.ph/data-privacy-act/

National Privacy Commission (NPC). (2017). NPC survey: Filipinos value data privacy. https://www.privacy.gov.ph/2017/08/npc-survey-filipinos-value-data-privacy/

University of the Philippines (UP). (2019). UP forum roundtable discussion: What do you understand about the Data Privacy Act of 2012? What do you do to protect your data? https://up.edu.ph/up-forum-roundtable-discussion-what-do-you-understand-about-the-data-privacy-act-of-2012-what-do-you-do-to-protect-your-data/

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494-620. https://doi.org/10.7916/cblr.v2019i2.3424

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. Communications in Information Literacy, 11(2), 378-389. https://eric.ed.gov/?id=EJ1166461