University Students' Awareness and Attitudes Towards Data Privacy in a Digital Age

Ishika Khatri
Mittal School Of Business, Lovely Professional University Jalandhar, Punjab
ishikakhatri11.11@gmail.com

Simran Kashyap
Mittal School Of Business, Lovely Professional University Jalandhar, Punjab
simkash@gmail.com

Mohammad Khalid Raza
Mittal School Of Business, Lovely Professional University Jalandhar, Punjab
ramohammadkhalid@gmail.com

Ridhi Kumari
Mittal School of Business, Lovely Professional University
Jalandhar, Punjab
ridhik74@gmail.com

Arun Kaushal (Assistance professor)
Mittal School of Business, Lovely Professional University
Jalandhar, Punjab
arunmonu.kaushal11@gmail.com

Abstract—In this study, the awareness and attitude of college students towards data privacy in the digital era are examined. The quantitative method applied in data collection was descriptive and cross-sectional, whereby undergraduate and graduate students were administered an online questionnaire. The findings indicate that despite the moderate level of knowledge about data privacy concepts and risks, students do not necessarily show cautious online behavior. The privacy paradox is also manifested in the fact that most students continue to share personal information despite the privacy issues. Another aspect that is highlighted in the study is the effect of perceived risk and trust in digital platforms on privacy attitudes and data-sharing behavior. The findings indicate the need to have behavior-oriented, practical data privacy education.

Index Terms—component, formatting, style, styling, insert.

I. INTRODUCTION

Data privacy is a global trend that is especially affecting young adults who are the most active and pioneers of digital media. University students represent a significant and distinct segment of the larger population of young adults; their daily lives are highly connected with various applications of online services to academic research, personal communication, entertainment, and social networking. Due to the constant consumption of digital services by the students, they are not only active members of very complex data ecosystems, but also contributors to, and even victims of, the same ecosystems. A vast amount of personal information is being systematically gathered, stored, processed, and, more and more, manipulated in every one of these very large-data systems.

The pace of technological change (such as: the emergence of mobile applications; the development of cloud computing; and the manner in which we create and consume personal information) is providing novel methods of doing things. This fast change begs the question: who owns digital information; who has sufficient protection of their digital information; do people have full knowledge of their legal rights and responsibilities of their digital information. College students are often called digital natives and are presumed to be well versed with the digital world today, yet numerous studies have indicated otherwise.

The blistering development of digital technologies has changed the process of creating, collecting, storing, and commercializing personal data radically. University students can be referred to as digital natives because they are one of the most active users of social media platforms, learning management systems, cloud services, online banking applications, and AI-driven digital tools. The issue of personal data security, privacy rights, and algorithmic surveillance has grown with the growing intensity of data in digital ecosystems (Acquisti et al., 2015). The introduction of big data analytics, artificial intelligence, and predictive algorithms into the daily platform has transformed the decision-making process that is to be applied to the environment controlled by the

user into the algorithm-based system where the data transparency is frequently restricted. The academic literature on digital privacy has grown immensely over the last ten years in information systems, marketing, cybersecurity, behavioral economics, and education. The initial research was mainly focused on the technical security controls and legal compliance requirements like the General Data Protection Regulation (GDPR). Nevertheless, more recent sources have moved to the psychological aspect of privacy, such as perceived risk, trust in online services, and the so-called privacy paradox, the discrepancy between the stated privacy concerns and the actual online behavior (Barth & de Jong, 2017). This contradiction is especially evident in younger generations that are sensitive to the threat of privacy and share personal information on online platforms on a large scale. Digital learning systems, AI-based analytics, and data-driven personalization tools have only added to the privacy situation in the context of higher education. To improve the learning process, track student engagement, and personalize academic services, universities are becoming more and more dependent on student data. Although these technologies have advantages in terms of operations, they also have ethical and governance issues related to consent, transparency, and institutional accountability, (Soffer, 2024). The literature is biased to address individual elements of privacy awareness, trust, or behavioral intention, but the gap in the literature is the absence of the evaluation of the overall impact of data privacy awareness on student attitudes and actual data-sharing behavior. Although there is an increasing empirical interest, the literature remains silent on the systematic study of the interaction between awareness and trust and perceived risk to influence behavioral outcomes among university students. Most studies presuppose that the more the awareness, the more careful the digital behavior. However, empirical evidence has demonstrated that awareness might not be enough to lead to significant behavioral changes, (Kokolakis, 2017). The relationship between awareness, attitudes, trust in digital platforms, and data-sharing behavior is thus important to learn in order to develop effective privacy education programs and institutional policies. To fill this gap, the current research will be quantitative, cross-sectional to examine the awareness and attitude of university students towards data privacy in the digital era. The research aims to bring empirical clarity to the understanding of the student privacy choice processes by incorporating the privacy awareness, perceived risk, trust, and data-sharing behavior constructs.

The research questions in this study are as follows:

RQ1: What is the existing level of data privacy awareness among university students in the online space?

RQ2: What is the relationship between the trust in digital platforms and perceived risk of privacy and the attitude of students towards data privacy?

RQ3: Does data privacy awareness have a significant effect on data-sharing behavior of students or is the privacy paradox existent despite awareness? The research will add to a more systematic knowledge of student-centered digital privacy behavior by the empirical investigation of these relationships. The results will be used to educate universities, policymakers, and designers of digital platforms to create some awareness campaigns that are not diminished to the dissemination of information but also promote responsible digital decision-making.

A. Objectives of the Study

• Survey of the current level of awareness of university students regarding the fundamentals of data privacy, the relevant laws and regulations regarding the same issue, and the new digital threats.

The study will involve the attitude analysis of university students regarding data privacy. The areas of interest will be online trust, perceived value of data, and institutional accountability.

• Exposition of some of the actions and mental orientations of university students that provide protection of privacy.

•Identification of demographic and academic variables (field of study and age) that contribute to the degree of awareness and general attitude of a student.

• Development of specific recommendations to improve the education of data privacy and institutional data policy within a post-secondary institution.

B. Scope and Limitations

The study will target undergraduate and graduate students of Indian universities that are involved in the project. The research design will be to conduct large scale surveys to gather both quantitative and qualitative information regarding student attitude towards privacy.

The study will be limited in a number of ways. Response bias due to self-reported data is possible. The high rate of technological change will affect the duration of relevance of the results. The geographical and institutional nature of the study will also restrict the extrapolation of the results to a global setting.

II. REVIEW OF LITERATURE

B.G.Mujtaba [1] Examined Human-AI Intersection: Understanding the Challenges, Opportunities, and Governance Protocols to a Changing Data-Driven Digital

World, which is concerned with the growing influence of artificial intelligence on contemporary organizations and societies. The paper emphasizes the high potential of AI to improve productivity, transparency, and ethical decision-making in all industries, and at the same time, it raises serious issues regarding the bias of algorithms, data privacy, and ethical governance. Summarizing a broad body of literature on AI ethics and its effects on society, the author highlights that it is essential to have responsible governance structures, clear system design, and AI literacy among the general population. The paper concludes by stating that AI should be created and implemented in a way that it can positively impact social well-being instead of supporting the status quo.

M. Paludi [2] discussed the topic of Safeguarding Privacy and Data Protection Rights in AI-Enhanced Education and Learning Analytics, specifically in the context of secondary school educational settings. The research explains the way in which the rights to privacy and the protection of personal data must be understood in the context of the introduction of artificial intelligence tools into the formal learning environment. Based on the legal frameworks, including GDPR and the EU AI Act, and the research on technology-enhanced learning, the author finds the gaps in digital and legal literacy of teachers and students. The research emphasizes that the interdisciplinary cooperation, enhanced teacher education, and specific awareness campaigns are necessary to make the AI-based learning analytics ethical, legal, and transparent.

Ria Ghosh, Meetu Malhotra, and Naresh Kumar [3] explored the topic of Cyber Bullying in the Digital Age: Challenges, Impact, and Strategies to Prevent it, and how anonymity and constant online connectivity contribute to the escalation of cyberbullying behavior. The paper describes the severe psychological, academic, and social impacts on victims. The authors highlight that technical solutions are not enough through a synthesis of the world research findings and intervention strategies. They present the argument of a concerted effort that incorporates education, enforcement of policies, parental and community involvement in order to build safer and more inclusive digital spaces.

Olayemi Timothy Adekeye and others [4] studied Vaping in the Digital Age: The Impact of Social Media on Adolescent Attitudes and Beliefs about E-Cigarette Use. The results indicate that social media networks often depict vaping as cool, socially acceptable, and harmless, which enhances the interest and exploration of adolescents. Attitudes are highly influenced by influencer endorsements and peer-generated content and health-risk messaging is relatively small. The paper concludes that more stringent digital advertising policies, more powerful public health campaigns, and increased digital health literacy are needed to combat misleading online stories.

G. Biagini [5] has carried out a systematic review, entitled Towards an AI-Literate Future: Exploring Education, Ethics, and Applications, which explores the conceptualization of AI literacy in educational settings. The review shows that AI literacy is not only technical but also moral and ethical, as well as critical thinking about AI systems. Through a wide range of international literature, the research finds that AI literacy programs are rapidly expanding, especially in technologically developed areas. Nevertheless, the author points out the necessity of culturally inclusive studies, longitudinal studies, and standardized assessment frameworks.

K. Maguraushe [6] suggested A Personal Information Privacy Perceptions Model to University Students, which attempts to describe the perception of students towards data privacy in academic institutions. The results show that institutional data practices trust, policy transparency, and perceived control have a significant impact on student acceptance of digital technologies. The interpretation of privacy risks is also influenced by cultural background. The paper concludes that privacy issues can be minimized through effective communication and transparency, but institutional and resource constraints may limit the implementation.

M. b. Kwapisz [7] studied Privacy Concerns of Student Data Shared with Instructors, which is concerned with how students perceive academic data access and use. The research concludes that ambiguous purposes of data use and the fear of academic repercussions increase privacy concerns. The author uses qualitative interviews to determine the anxieties associated with surveillance, unauthorized access, and the use of secondary data. The study suggests open consent procedures and access control (role-based) to enhance trust and ethical data management.

O. Viberg and colleagues [8] investigated the Cultural Differences in Privacy Concerns of Students in a multi-country survey. The results indicate that the attitudes towards privacy differ greatly in terms of cultural and national backgrounds and are strongly associated with institutional trust. High-trust students are more willing to provide data in exchange of education. The paper posits that privacy policies and educational interventions should be culturally sensitive and not standardized.

T. Soffer [9] explored Students Perceptions of Using Learning Analytics in Higher Education, exploring the ways students weigh the benefits of pedagogy against the dangers of privacy. The results show that the students appreciate the personalized learning support but are still

worried about transparency, accuracy of the data, and the use of algorithms to make decisions. The paper highlights the need to engage students in governance debates and explain the working of analytics systems in a clear manner to establish trust.

Student Attitudes, Awareness, and Perception on the Use of social media and Data Privacy were studied by J. N. A. Sales [10], and the privacy paradox remains. Even though students are expressly aware of the dangers of privacy, convenience frequently causes them to engage in risky behaviors. The research suggests digital literacy programs that emphasize on practical, easy to adopt privacy practices and privacy-by-default system designs to close the awareness-behavior gap.

Nongkhai, Wang, and Mendori [11] suggested an Ontology Based Adaptive Learning System of Programming Education, which is aimed at personalizing the teaching of coding. The system combines semantic knowledge representation with performance tracking of the learners to dynamically adjust the content. The results show better interaction and learning of basic programming subjects. Nevertheless, the authors admit the scope limitations and propose the extension of the framework to the advanced programming skills.

Fokou Pelap, Fitime and Mbaiossoum [12] introduced Ontology-Based Learner Modeling of Personalized eLearning Systems, which emphasized on structured descriptions of learner attributes, including skills, preferences, and cognitive styles. The framework facilitates dynamic content presentation and analytics of learning. Although the study is conceptually sound, it is not empirically validated, which makes it a basis of applied research in the future.

Ivanova [13] studied Semantic Personalization with Concept Maps, Knowledge Graphs, and Ontologies in Adaptive Learning. The paper explains the use of a combination of semantic tools to improve individual feedback and student comprehension. The ability to interoperate between cognitive and semantic models is emphasized as one of the key strengths. Nevertheless, the lack of quantitative analysis restricts the empirical contributions of the study.

Dong and co-authors [14] suggested a Knowledge Graph-

Improved AI Tutoring System with Retrieval-Augmented Generation. The hybrid model bases generative AI responses on structured domain knowledge, which results in better learner performance and flexibility. The paper focuses on improved explainability but observes that the effectiveness of the system is strongly determined by the quality and completeness of the underlying knowledge graph.

Chen, Saeedvand, and Lai [15] explored Adaptive Learning Path Navigation with Reinforcement Learning and Knowledge Tracing. They dynamically adapt learning sequences to predicted states of the learners. The results show greater interaction and learning effectiveness. Nevertheless, low interpretability and semantic grounding are still issues.

Anindya Roy and Aaron Kessler [16] investigated How College Students Feel About Data Privacy and the Data Economy, discussing the attitude of students towards the collection of personal data. The results indicate that there is an unease with the large-scale use of corporate data even though they often use technology. The research points to the lack of awareness of privacy legislation and recommends the inclusion of data privacy education in technical programs.

The SPICE Model of Privacy Concerns in Learning Analytics among Students was created by Chantal Mutimukwe and others [17]. The model describes the relationship between perceived privacy risk and perceived control and trust and willingness to share data. The research determines privacy risk as the most significant determinant of concern and highlights clear policies and participatory system design.

Anjuman Ara, Zuradiah Zainol, and Balagasen Duraisamy [18] studied the Effects of Privacy Awareness, Security Concerns, and Trust on Information Sharing in social media. The results show that the greater the privacy awareness, the less information is shared, and the greater the trust, the more willing to share data. The paper emphasizes the significance of effective security controls and clear privacy policies.

Manh-Tung Ho and colleagues [19] investigated Gen Z Attitudes Towards Emotional AI and Non-Conscious Data Collection. The cross-cultural analysis shows that the level of acceptance differs greatly depending on demographic, cultural, and socio-political factors. The authors criticize the conventional technology acceptance theories and highlight the necessity of culturally sensitive AI governance.

C¸ agdas¸ Umit [20] examined the Relationship Between Online Privacy Concerns and Internet Addiction Among University Students. The research concludes that there is a positive relationship between high internet use and increased privacy anxiety. The levels of concern are also

affected by gender differences and patterns of platform use. The study identifies the privacy paradox, which is the presence of concern and risky online behavior.

III. SUMMARY TABLE

TABLE I

AUTHOR	TITLE	KEY FINDINGS	REVIEW INSIGHTS
Mujtaba	Human–AI Intersection	Efficiency with ethical risks	Governance needed
Paludi	AI & Privacy in Education	Legal and literacy gaps	Ethical safeguards
Ghosh et al.	Cyber Bullying	Psychological harm	Multi-stakeholder role
Adekeye et al.	Vaping & Social Media	Online normalization	Regulation required
Biagini	AI Literacy	Ethics beyond technology	Standardization needed
Maguraushe	Privacy Perception Model	Trust and control matter	Transparency critical
Kwapisz	Student Data Privacy	Fear of misuse	Consent mechanisms
Viberg et al.	Cultural Privacy	Cultural differences	Localized policy
Soffer	Learning Analytics	Benefits vs. privacy risk	Student involvement
Sales	Privacy Awareness	Privacy paradox	Digital literacy
Nongkhai et al.	Adaptive Learning	Improved engagement	Limited scope
Fokou Pelap et al.	Learner Modeling	Personalization potential	Needs validation
Ivanova	Semantic Learning	Improved feedback	Theoretical focus
Dong et al.	KG–RAG Tutor	Explainable AI	Data dependent
Chen et al.	Adaptive Paths	Learning efficiency	Low interpretability
Roy & Kessler	Data Economy	Student discomfort	Policy awareness
Mutimukwe et al.	SPICE Model	Risk affects trust	Empirical strength
Ara et al.	Privacy & Trust	Trust boosts sharing	Security needed
Ho et al.	Emotional AI	Cultural variation	Governance focus
Yazgan	Privacy & Internet Addiction	Privacy anxiety linked to excessive use	Privacy paradox evident

IV. Objectives of the Study

1. To investigate the degree of data privacy awareness among university students in terms of personal data collection, use, and protection in the digital space.

2. To examine the attitudes of students towards data privacy, their perception of privacy rights, transparency, and institutional responsibility.

3. To examine how perceived risks of privacy affect the online behaviour and decision-making of students concerning data sharing.

4. To determine the importance of trust in digital platforms and institutions in determining willingness of students to share personal information.

5. To determine the prevalent risky online behaviours among university students, including oversharing on social media, giving too many apps permissions, and ignoring privacy settings.

6. To investigate the existence of the privacy paradox in university students by looking at the discrepancies between their expressed concerns and their real online actions.

7. To determine the influence of digital literacy and awareness rates on the use of privacy-protective practices by students.

8. To investigate how institutional and legal frameworks (including GDPR and DPDP Act 2023) can affect the knowledge of students about their rights to data privacy.

9. To examine the correlation between data privacy awareness, attitudes, trust, perceived risk, and data-sharing behaviour among university students.

10. To offer evidence-based recommendations to the universities, policymakers and digital platforms on how to improve data privacy awareness and encourage responsible digital practices among students.

V. RESEARCH METHODOLOGY

A. Research Design

The study employs a descriptive, cross-sectional, and analytical study design to examine the knowledge and perceptions of university students on data privacy in online settings. The descriptive part of this research determines the level of awareness of university students regarding their personal data usage, the possible privacy threats, and the way they secure their own data online. The cross-sectional aspect of the research will entail the gathering of data on people at a single point in time, such that the researchers will be in a position to describe the current perceptions, beliefs, and behaviors regarding data privacy without following any changes in the same over time. Lastly, the analytic component of this project will enable the researchers to investigate the connection between awareness, beliefs, trust, and behaviors associated with data sharing.

The two qualitative research methods are used in this project since they offer the researcher a systematic way of quantifying the perceptions of the students, their beliefs, in terms of numerical measures. The qualitative methodologies have been applied widely in the past when exploring the problem of digital privacy and the behavior of university students since they enable the objective comparison of the responses of all the participants (i.e., university students), and they can be subjected to statistical analyses. Moreover, the survey method appears to be suitable considering the number of the university students, and the heterogeneity of the student population.

B. Research Approach

The two qualitative research methods are used in this project since they offer the researcher a systematic way of quantifying the perceptions of the students, their beliefs, in terms of numerical measures. The qualitative methodologies have been applied in the past when exploring the problem of digital privacy and the behavior of university students due to the fact that they enable the objective comparison of the responses of all the participants (i.e., university students) and are subject to statistical analyses. Moreover, the survey method appears to be suitable, considering the number of students in the university population, and the heterogeneity of the population.

C. Population of the Study

The sample consisted of all bachelors and master's degree students who are enrolled in a university/college. They all use various forms of digital media on a frequent basis like, Learning Management Systems (LMS), social media, online banking applications and cloud storage and thus, this is an appropriate sample population to examine their awareness of data privacy and their attitudes towards it.

D. Sampling Technique

Convenience sampling will be used to select respondents to give sufficient representation of this study. The convenience sampling will be employed because of time constraints, accessibility, and availability of respondents. Only willing respondents are included in the study and those that the researcher can easily access. This approach is acceptable in academia as far as perception-based studies are concerned, although it does restrict the generalizability of the study findings.

E. Data Collection Methods

1) Primary Data: The primary data collection in this study has been done by administering a structured online questionnaire. The data collection method (through the internet) has the merits of being cheap and the respondents can remain anonymous when addressing issues that are especially sensitive like being concerned about data privacy. The information was gathered on online platforms and submitted in electronic format.

2) Secondary Data: The secondary data of the study is acquired in the form of academic journals, conference proceedings and research articles mainly via Google Scholar. The secondary data is aimed at giving a theoretical framework of the data and assist in the interpretation of the primary data outcome.

F. Research Instrument (Questionnaire Design)

The questionnaire will be split into five parts:
1) Section A: Demographics, age, gender, and educational level/field of study.
2) Section B: Understanding of Data protection concepts such as personal data, data consent and the way people use data.

3) Section C: Data protection attitudes and concerns about the collection of digital data on consumers.
4) Section D: Perceived risk of privacy and dependence on the digital platforms.
5) Section E: The data-sharing habits of students, and their consumer privacy care practices.

G. Measurement Scales

The respondents will be asked to respond to Likert-scale statements to give a systematic means of expressing their degree of awareness/attitude to certain concepts. There were multiple-choice questions to determine behavior patterns. The research does not use open-ended questions to increase reliability and enhance the consistency of analysis.

H. Variables of the Study

The following key variables are the subject of this study:

1) Data privacy awareness
2) Perceptions of data privacy.
3) Perceived privacy risk
4) Trust in digital platforms
5) Data-sharing behavior

These variables were determined based on the similar themes that were present throughout the literature on student data privacy and digital behavior.

I. Validity and Reliability

1) Validity: Content validity Questionnaire items are based on content that has been developed in previous research studies, and are reviewed to determine the clarity and relevance of items. Pilot test is also conducted to determine ambiguities/unforeseen findings of previous studies and changes made according to the pilot testing feedback.

2) Reliability: Reliability of the instrument is established by using Internal Consistency measures (e.g. Cronbachs alpha) where necessary. This gives confidence that the items to be used to measure a given variable will yield consistent/reliable results.

J. Data Analysis Techniques

The survey data was collected and analyzed using simple statistical techniques. Descriptive statistics (e.g., percentages, means and standard deviations) will be used to summarize the demographic and awareness level data. The data will be clarified visually with the help of different graphical representations (e.g., bar Graph/Bar Chart, Pie Graph/Pie Chart). Besides descriptive statistics, correlation analysis will also be conducted to examine the relationships between the levels of awareness, levels of trust, and attitudes towards data privacy, respectively.

H. Ethical Considerations

The study has followed rigorous rules of ethical behavior throughout. Every participant was made aware of the nature of the research before filling their survey/questionnaire. The personal identifying information of the participants was safeguarded; hence, they were anonymous and confidential. The data gathered will be utilized solely in education.

A. Scope and Limitations

The study will include university students as the only participants and will focus on the awareness and attitudes of university students regarding data privacy in a digital world. The study does not include any analysis of the various technical safeguards or legal enforcement mechanisms applicable to data privacy issues. The study's limitation includes reliance on the participants' self-reporting, a small sample population, and the use of non-probability sampling; however, the study's design and implementation provide important information regarding university students' perceptions of data privacy issues.

VI. RESEARCH GAP

Research conducted to date about data privacy by college-age people (university students) has measured three primary aspects: levels of awareness (of issues regarding data privacy), privacy concerns (how much concern there is about data privacy) and perceived risks (how risky people view sharing their data). Most studies investigating these variables typically assume that a higher level of awareness about data privacy issues translates into a more cautious approach to data sharing and more responsible behavior with respect to sharing their data.

Accordingly, awareness of data privacy issues is generally viewed as being sufficient for creating better privacy outcomes. However, very few studies empirically evaluate the extent to which university students' awareness of data privacy affects their attitudes and actual decision-making behavior relative to their daily life experiences in the digital realm. While university students may have some level of awareness of privacy risks, regulations, or threats, there has been little, if any, research that actually examines whether university students consider their data privacy awareness when making everyday decisions (e.g., agreeing to terms of service for an online platform, granting permission to use an application, or sharing his/her information online).

Similarly, although the privacy paradox (where people express concern for privacy but still share their information) has been often documented, many studies merely describe these two concepts but do not attempt to explain how the lack of action stems from a lack of translation from data privacy awareness to action. As such, additional research is needed to assess how data privacy awareness affects

(1) university students' attitudes, (2) university students' trust, and (3) university students' actual data-sharing behavior within a given digital environment (whether the environment is real or virtual).

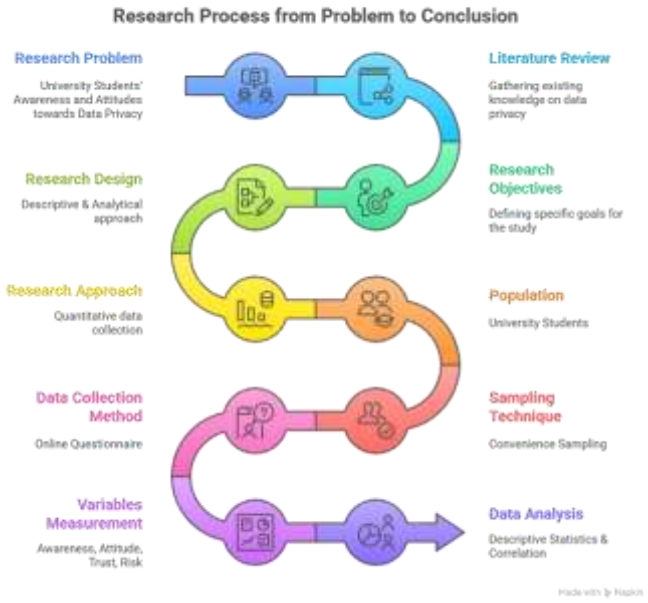


Fig. 1. Research process from problem identification to conclusion

In this regard, there is a significant research gap in the sense that no empirical studies have been conducted to combine a student-centered approach to determine whether or not and how data privacy awareness has affected the attitudes of university students towards data privacy and their readiness to give personal data in the digital world. It is the responsibility of researchers to fill this gap so that they can come up with effective awareness programs and the institutional policies that accompany them, and privacy education programs of such a nature that will not only impart information but will also result in a behavior change that can be demonstrated.

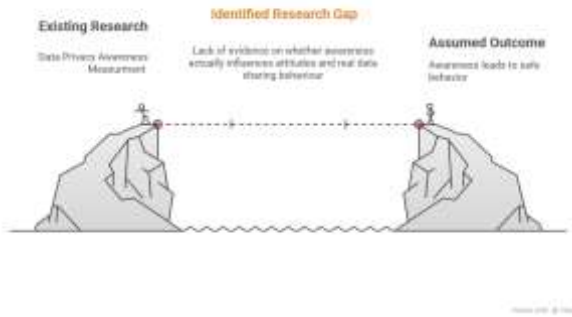


Fig. 2. Conceptual representation of the identified research gap and the proposed study outcome

VII. RESEARCH HYPOTHESES

H1 - The more students know about the gathering and use of their personal data, the more likely they are to value and appreciate data privacy.

H2 - Students with a high level of data privacy tend to be cautious when sharing their personal data on online platforms.

H3 - The level of student confidence in online platforms, and their perceptions regarding the dangers of data misuse, will determine the extent to which the problem of data privacy awareness will impact their attitudes.

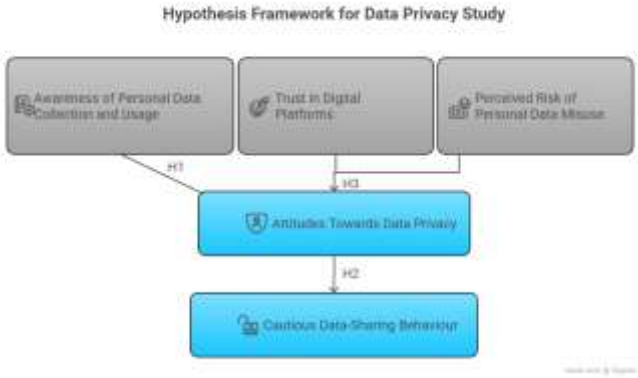


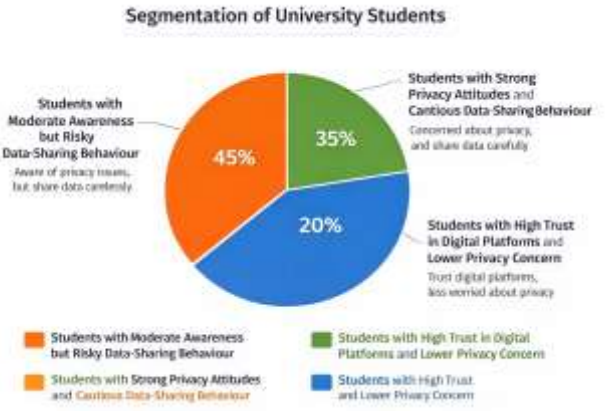
Fig. 3. Hypothesis framework of key factors influencing data privacy attitudes and data-sharing behavior.

VIII. CONCLUSION

The study examined the awareness and attitudes of university students on data privacy in the digital era using a descriptive cross-sectional research design. The findings revealed that the majority of the respondents exhibited moderate awareness of personal data collection, privacy threats, and digital data use.

Although there was awareness, there was inconsistency in the responses in showing cautious online behavior. The percentage of respondents who shared personal data despite being aware that there was a possibility of privacy concerns was high. Even though a significant number of students expressed their concern about their data privacy, only a few of them used strong privacy protection behaviors (e.g., restricting data sharing, changing privacy settings)

This observation shows that the privacy paradox still exists among university students. The results indicate that universities and policymakers should not only focus on awareness-based programs but also devise strategies that will enable students to use their knowledge on privacy in their daily digital decision-making. Although this study had its limitations (e.g., self-reported data and cross-sectional design), it offers useful information about the current student perceptions and behaviors in terms of data privacy. Longitudinal studies or comparative studies across institutions would give more information on how the awareness, attitudes and behaviors of students towards data privacy evolve over time.



IX. Future Scope

Although the current research offers a lot of information on the awareness and attitude of university students towards data privacy in the digital era, there are still a number of opportunities that can be explored in future studies. To begin with, the longitudinal research design can be used in future research to investigate the changes in the awareness, attitudes, and data-sharing behaviours of students as they mature and become more exposed to digital platforms, technological innovations, and privacy policies. This would offer more information on causal relationships and behavioural changes than cross-sectional analysis can offer.

Second, the geographical and institutional scope of the study can be extended in future studies by incorporating students of various universities, regions, and cultural backgrounds to increase the generalizability of the results. International comparisons can also be used to shed more light on how regulatory systems, digital literacy, and cultural aspects affect student perceptions and behaviours regarding privacy.

Third, future research can use mixed-method designs by integrating quantitative surveys with qualitative research methods like interviews or focus groups to understand the motivations, perceptions, and experiences of students regarding data privacy in more detail. This would give deeper contextual insight than statistical analysis.

Fourth, further studies can be conducted to investigate other variables like personality traits, dependence on technology, academic discipline, and level of digital literacy to gain a better understanding of their impact on privacy awareness and behaviour. The combination of psychological and behavioural constructs can reinforce theoretical explanations of the privacy paradox among students.

Fifth, new technologies like artificial intelligence, biometric systems, learning analytics platforms, and generative AI tools introduce new privacy issues that should be further empirically explored. Further studies can be conducted in particular to investigate how students perceive AI-based data collection, automated decision-making, and algorithmic transparency in schools.

Lastly, the future research can be aimed at assessing the efficacy of specific digital privacy education initiatives, awareness campaigns, and institutional policies in enhancing responsible online behaviour among students. Intervention or experimental research designs may offer viable suggestions to universities, policymakers, and developers of digital platforms.

In general, the broadening of research in the methodological, geographical, technological, and behavioural aspects will help to understand student data privacy in the fast-changing digital ecosystem more thoroughly.

X. REFERENCES

[1] Mujtaba, B. G. (2025). Human-AI Intersection: Learning the Ethical Iss, Opportunities, and Governance Procedures of a Shifting Data-Driven Digital World. Business Ethics and Leadership, 9(1), 109126.

[2] Paludi, M. (2025). Protecting Privacy and Data Protection Rights in AI Enhanced Education and Learning Analytics: An Interdisciplinary.

Instruction in Secondary High School Learning Centers. Dalam Ortega-Arranz A., McLaren BM, and Buchem I. In CEUR Workshop Proc (Vol. 3927, pp. 83-89).

[3] Ghosh, R., Malhotra, M., & Kumar, N. (2025). Cyber Bullying in the Digital Age: Problems, Effect, and Prevention. In Fighting Cyberbullying with Generative AI (pp. 151-180). IGI Global Scientific Publishing.

[4] Adekeye, O. T., Boltz, M., Jao, Y. L., Branstetter, S., and Exten, C. (2025). Vaping in the digital era: The role of social media in shaping adolescent attitudes and beliefs towards the use of e-cigarettes. Journal of Child and adolescent Substance Use, 30(1), 13-26.

[5] Biagini, G. (2025). Towards an AI-Literate Future: A systematic literature review of education, ethics, and applications. International Journal of Artificial Intelligence in Education, 1-51.

[6] Maguraushe, K. (2024). A model of personal information privacy perceptions among university students. Education and Information Technologies, 29(4), 45674585.
https://www.tandfonline.com/doi/full/10.1080/19393555.2024.2329554# abstract

[7] Kwapisz, M. B. (2024). Student data privacy with instructors. ACM on Human-Computer Interaction, 8(CSCW1), 125.
https://dl.acm.org/doi/pdf/10.1145/3613904.3642914

[8] Viberg, O., Khalil, M., & Baars, M. (2024). The privacy concerns of students in different cultures: A cross-country survey. Computers & Education, 201, 104789.
https://arxiv.org/abs/2312.02093

[9] Soffer, T. (2024). The perception of students towards the use of learning analytics in higher education: The trade-off between benefits and privacy risks. Australasian Journal of Educational Technology, 40(1), 4560.
https://ajet.org.au/index.php/AJET/article/view/9130/2149

[10] Sales, J. N. A., & Cruz, R. M. (2024). Attitudes, awareness, and perceptions of data privacy on social media platforms among students. International Journal of Information Management, 75, 102682.
https://ijci.net/index.php/IJCI/article/view/1398/710

[11] Nongkhai, L. N. A., Wang, J., & Mendori, T. (2023). Ontology-based adaptive learning support system. Proceedings of the 31 st International Conference on Computers in Education (ICCE 2023).
https:/ doi.org/10.58459/ icce.2023.958.

[12] [Fokou Pelap, G., Fippo Fitime, L., & Leouro MBAIOSSOUM, B. (2023). Ontology-based modeling of the learner in a web educational system: Towards learning analytics and adaptive learning. International Journal of Innovative Science and Research Technology, 8(7).
https://doi.org/10.5281/zenodo.8202235

[13] Ivanova, T. (2023). Knowledge graphs, concept maps, ontologies and intelligent semantics-based methods of personalized learning. In EDULEARN23 Proceedings (pp. 6266–6275).
https://doi.org/10.21125/edulearn.2023.1654

[14] Dong, C., Yuan, Y., Chen, K., Cheng, S., and Wen, C., (2023). Building an adaptive AI tutor in any course with knowledge graph-enhanced retrieval-augmented generation. arXiv preprint arXiv:2311.17696.
https://arxiv.org/abs/2311.17696

[15] Chen, J.-Y., Saeedvand, S., & Lai, I.-W. (2023). Knowledge tracing-based adaptive learning path navigation with reinforcement learning. arXiv preprint arXiv:2305.04475.
https://arxiv.org/abs/2305.04475

[16] Roy, A., & Kessler, A. (2022, August). The attitudes of college students towards data privacy and the data economy. In Proceedings of the 2022 ASEE Annual conference and Exposition. American Society of Engineering Education.

[17] Mutimukwe, C., Viberg, O., Oberg, L. M., and Cerratto-Pargman, T. [17]. Privacy concerns of students in learning analytics: Model development. British Journal of Educational Technology, 53(4), 93295.

[18] Ara, A., Zainol, Z., & Duraisamy, B. (2022). The influence of privacy awareness, security issues, and trust on information sharing in social media among public university students in Selangor. International Business Education Journal, 15(2), 93110.

[19] Ho, M. T., Mantello, P., Ghotbi, N., Nguyen, M. H., Nguyen, H. K. T., and Vuong, Q. H. (2022). Reconsidering technological acceptance in the era of emotional AI: Gen Z (Zoomer) attitudes towards nonconscious data collection. Technology in Society, 70, 102011.

[20] Yazgan, C¸. U. (2022). Exploration of the connection between online privacy issues and internet addiction among college students.

Journal of Media and Religion Studies, 5(1), 6177.