Scientific and Practical Cyber Security Journal (SPCSJ) 9(1): 10 – 20 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

PRIVACY CONCERNS IN FACIAL RECOGNITION TECHNOLOGY AT A HIGHER PRIVATE EDUCATION INSTITUTION IN SOUTH AFRICA

Nozipho Nhlapho[1] and Brian Maodza[1]
The Independent Institution of Education[1]

ABSTRACT: There is a growing trend of implementing facial recognition technology (FRT) in higher education institutions to enhance security and administrative functions. However, this technology raises significant privacy concerns regarding the protection of personal data. This study examined students' privacy concerns related to the use of FRT at a private institution in South Africa. Although FRT improves safety, it introduces notable privacy risks that current safeguards fail to fully address. The research focused on student concerns about the collection, storage, and use of their facial recognition data. A survey using stratified random sampling was conducted with 106 participants to assess their perceptions of their privacy in relation to facial recognition technologies and how their data is safeguarded against disclosure. The findings revealed significant privacy concerns and scepticism about the adequacy of current safeguards from the students. These results contribute to the ongoing debate on balancing technological advancement with individual privacy and suggest ways to improve privacy measures in FRT systems.

KEYWORDS: *Facial recognition technology (FRT), Privacy Concerns, Higher Education Institutions, Consent, Privacy Safeguards, Student Attitudes*

1. INTRODUCTION

Facial recognition technology is commonly used to increase safety measures and optimize operational efficiency in higher education institutions. Privacy refers to an individual's ability to have control over the access of their personal information for example facial data, name, date of birth, ID number etc. (Meden, B., et al, 2023). Facial Recognition Technology uses modern algorithms to identify and authenticate individuals through the study of facial traits from videos or photos (Wang et al., 2024).

Facial recognition technologies are utilized in various settings such as schools and higher education campuses to streamline processes and to enhance safety of students and staff (Wang et al., 2024). The widespread use of facial recognition technologies has raised significant concerns about privacy, prompting a thorough examination of its implications (Roundtree, 2023). The use of facial recognition technology (FRT) in private higher education institutions in South Africa has raised major privacy concerns (Meden et al., 2021). These concerns revolve around data ownership and its impact on student privacy as institutions may collect and distribute large amounts of data without obtaining student consent (Gies et al., 2020).

Without proper protections, students' personal information could be shared without permission, eroding trust. The aim of this research is to comprehend the privacy concerns of using facial recognition technology at a private higher education institution in South Africa. The study examined the perceptions of students on the use of facial recognition technology at a private higher education institution in South Africa., to grasp the ethical, legal, and societal implications at play. The following sub sections briefly presents the problem statement, research questions and objectives of the study.

1.1 Problem Statement:

FRT is increasingly used in higher education, primarily for campus security, but its widespread adoption raises serious privacy risks (Sarabdeen, 2022). In the U.S., schools spend $2.7 billion annually on security due to incidents like school shootings (Andrejevic & Selwyn, 2019). FRT systems help monitor campus access and activities (Andrejevic & Selwyn, 2019), but the data stored in FRT databases is

vulnerable to breaches and exploitation by unauthorized individuals (Liu et al., 2021). As these databases grow, the risk of security breaches increases, making them attractive to hackers (Liu et al., 2021).

The lack of comprehensive privacy guidelines in higher education exacerbates these risks. Policymakers must draft strong privacy regulations to safeguard individual rights and prevent misuse of FRT (Wu, 2024). These regulations should include informed consent, opt-out options, and clear data management protocols. Further research is needed to enhance privacy protections as technology evolves (Sciencebox.uz, 2024).

1.2 Purpose Statement:

This research aims to examine privacy concerns related to FRT use in a higher education institution, focusing on students' perspectives. A quantitative approach using questionnaires will be employed to gather data.

1.3 Research Questions:

1. What are the privacy concerns associated with the use of FRT in a higher education institution?
2. How effective are current privacy safeguards in protecting personal data within FRT systems?

1.4 Objectives:

1. To identify privacy concerns associated with FRT in a private higher education institution.
2. To evaluate the effectiveness of current privacy safeguards in protecting personal data within FRT systems.

2. THEORETICAL FOUNDATION

Understanding how to manage personal information is vital for privacy protection. (Petronio and Hernandez, 2002), proposed the Communication Privacy Management (CPM) theory. The theory outlines how individuals and groups handle the disclosure of personal information (Knijnenburg et al., 2022). This theory involves identifying ownership of personal information and establishing security guidelines (Lehmuskallio and Lampinen, 2019).

CPM scholars categorize rules related to private information into privacy boundaries, ownership, and sharing, which are essential for setting boundaries in organisations like private higher education institutions in South Africa (Lehmuskallio and Lampinen, 2019). The research applied CPM theory to explore students' privacy concerns regarding facial recognition technology. It aimed to understand how students perceive their privacy, navigate personal boundaries, and address ethical dilemmas posed by this technology (Petronio and Hernandez, 2019).

3. LITERATURE REVIEW ON FACIAL RECOGNITION TECHNOLOGY

This section reviews existing literature on facial recognition technology (FRT) and its implications for privacy, ethics, and societal values. The review will cover various aspects of FRT, including privacy concerns, the effectiveness of current regulations, data ownership and consent issues, surveillance practices, bias and discrimination, and strategies for ensuring privacy protection. Each of these subtopics will be discussed in detail in the following sections.

- 3.1: Privacy Concerns of Facial Recognition Technology
- 3.2: Effectiveness of Privacy Safeguards and Regulations
- 3.3: Data Ownership and Consent Issues
- 3.4: Surveillance and Monitoring
- 3.5 Bias and Discrimination
- 3.6 Strategies for Ensuring Privacy Protection

3.1 Privacy Concerns of Facial Recognition Technology

Facial recognition technology (FRT) has raised significant privacy concerns despite its benefits for security and convenience. Studies show that many individuals feel negatively about FRT, with 42% expressing discomfort due to its potential to invade privacy (Zhang, Feng, & Sadeh, 2021). Wu (2024) found that 91% of college students believe FRT significantly impacts their lives, further emphasizing privacy concerns. In schools, FRT is seen as infringing on freedom and privacy (Zeng et al., 2019). These concerns are often tied to the lack of transparency in how data is collected, stored, and used, leaving individuals feeling vulnerable to misuse. While research methods like surveys and interviews provide insights into these issues, they may not fully capture the complexity of public sentiment. For instance, Wu's (2024) app-based survey gathered data quickly but may have excluded nuanced feedback, highlighting the need for more comprehensive studies. Overall, the growing adoption of FRT underscores the importance of addressing privacy concerns to ensure ethical and responsible use.

3.2 Effectiveness of Privacy Safeguards and Regulations

Existing regulations for FRT have struggled to keep up with its rapid advancements, leaving gaps in privacy protections (Richardson, 2022). Current laws are insufficient in addressing misuse and breaches, with some arguing that they fail to fully safeguard individuals' privacy (Meden et al., 2021). Collaborative efforts between governments, industries, and institutions are necessary to enhance privacy safeguards and adapt rules to evolving technology. For example, Zeng et al. (2019) emphasize the importance of joint efforts to create robust frameworks that balance innovation with privacy protection. Higher institutions must proactively develop and enforce policies to address privacy concerns before they escalate. By fostering collaboration and updating regulations, organizations can create a more secure environment that aligns with technological advancements.

3.3 Data Ownership and Consent Issues

FRT raises questions about data ownership and consent, particularly in educational settings. Compliance with regulations like GDPR requires explicit consent but lacks clarity regarding its application to facial images (Steinacker et al., 2020). This ambiguity creates confusion about the type of consent required and who owns the data. Ethical challenges include safeguarding data, limiting collection, and ensuring anonymity. Students must be informed about how their data is used and given control over its usage, yet confusion around data ownership persists (Aswad & Marx Gómez, 2021). Additionally, debates about data retention, ethical use, and academic freedom further complicate the issue. Addressing these challenges requires clear policies and greater transparency to ensure that individuals' rights are protected while fostering trust in FRT systems.

3.4 Surveillance and Monitoring

FRT is increasingly used for surveillance in schools, leading to concerns about constant monitoring and its impact on student freedom. Studies highlight cultural differences, with extensive surveillance in China reducing acceptance of FRT, while it is more welcomed in Germany as a security measure (Kostka, Steinacker, & Meckel, 2020). In some cases, surveillance creates a tense atmosphere, as students feel they are constantly being watched and assessed, which can hinder their independence and learning experience. Conversely, in countries like Germany, FRT is perceived as a tool for enhancing safety and efficiency. These contrasting perspectives underscore the need to balance safety and privacy while considering cultural contexts. Schools must carefully evaluate the implications of surveillance to ensure it does not infringe on students' rights or create an oppressive environment.

3.5 Bias and Discrimination

FRT has been criticized for perpetuating bias and inequality. Studies show it often favours majority groups while misidentifying minorities, particularly women with dark skin (Venditti et al., 2019; Sarabdeen, 2022). This bias stems from a lack of diversity in training datasets, which can lead to inaccuracies and unfair treatment for marginalized groups. Additionally, engineers' cultural

perspectives can influence FRT accuracy, raising concerns about its fairness in multicultural societies like South Africa. These issues highlight the need for more inclusive and representative datasets to ensure equitable outcomes. Addressing bias in FRT is crucial for fostering trust and promoting social equity, particularly in diverse educational settings.

3.6 Strategies for Ensuring Privacy Protection in Facial Recognition Systems

To safeguard privacy, experts recommend transparent and ethical FRT regulations (Nesterova, 2020; McClellan, 2020). Empowering users with control over their data and employing advanced technologies, such as Support Vector Machines (SVMs), can enhance security while minimizing privacy risks (Mishra et al., 2023). Additionally, fostering accountability and inclusivity in the development of FRT systems is essential for ensuring ethical use. Schools and organizations must prioritize transparency, provide clear consent mechanisms, and adopt robust privacy safeguards to build trust and protect individuals' rights. By combining technological advancements with ethical practices, institutions can create a more secure and privacy-conscious environment.

4. RESEARCH DESIGN AND METHODOLOGY

4.1 Research Design and Population:

The research employed a cross-sectional approach, gathering data at a single point in time to understand students' attitudes and privacy concerns. The study targeted students aged 18–35 from a private higher education institution Campus in South Africa, chosen for its diverse student body. Participants represented various educational levels, fields of study, cultural backgrounds, and technological proficiency, ensuring a wide range of perspectives.

4.2 Sampling and Data Collection:

A stratified random sampling method was used to select 106 participants from different academic disciplines, ensuring fair representation. Data was collected through an online questionnaire distributed via QR codes and student platforms. The survey included Likert scale and multiple-choice questions to capture both quantitative data (e.g., privacy concerns) and demographic information. This method facilitated efficient and accessible data collection while encouraging high participation rates.

4.3 Data Analysis:

The study used statistical techniques, including descriptive statistics, crosstabs, and correlation analysis, to analyze the data. Descriptive statistics provided an overview of demographic distributions, while crosstabs examined relationships between variables like privacy concerns and fields of study. Correlation analysis explored connections between privacy concerns and perceptions of FRT. These methods offered insights into students' attitudes and privacy-related challenges.

4.4 Validity, Reliability, and Ethical Considerations:

To ensure reliability, the survey was pre-tested for clarity and accuracy, and a representative sample was chosen. Ethical considerations included obtaining informed consent, maintaining participant anonymity, and allowing voluntary participation. Transparency and fairness were prioritized throughout the study.

4.5 Limitations:

The study acknowledged limitations, such as its focus on a single institution, potential non-responses, and self-report bias. These factors may affect the generalizability of the findings. Efforts were made to minimize these issues by ensuring anonymity and encouraging honest responses.

5. FINDINGS AND INTERPRETATION OF FINDINGS

Upon conducting the survey and analyzing the data, a wealth of information was obtained regarding students' perceptions, attitudes, and experiences surrounding privacy and data handling in the institutional setting. This section delves into the key findings of the research, providing an in-depth examination of the data and its implications. A comprehensive analysis of the data revealed several pivotal insights, highlighting the complex relationships between privacy attitudes, perceptions of data handling, and various demographic factors.

Tab. 1. Crosstabulation of Privacy Implications Concern and Perceptions of Information Sufficiency

Privacy Implications Concern vs Sufficient information Crosstabulation

Count

		Sufficient information					
		Agree	Disagree	Neutral	Strongly agree	Strongly disagree	Total
Privacy Implications Concern	Agree	0	14	3	1	8	26
	Disagree	1	6	6	0	2	15
	Neutral	8	26	11	0	5	50
	Strongly agree	1	0	1	0	9	11
	Strongly disagree	0	0	2	0	2	4
Total		10	46	23	1	26	106

The crosstabulation results indicated a strong correlation between concerns about privacy and perceptions regarding the sufficiency of information provided by the institution. A significant majority of students who expressed worries about privacy also felt that the institution did not adequately communicate how their data was managed. Specifically, out of eighteen students expressing privacy concerns, 14 felt dissatisfied with the information provided. This finding supports the Communication Privacy Management (CPM) theory, which asserts that effective privacy management necessitates clear and sufficient information. The data suggest that inadequate information heightens privacy concerns among students, emphasizing the necessity for transparent communication regarding data handling practices. Previous research by Sarabdeen (2022) and Liu et al. (2021), reinforces the importance of effective communication in mitigating privacy concerns, showing that insufficient information can exacerbate anxiety around data misuse.

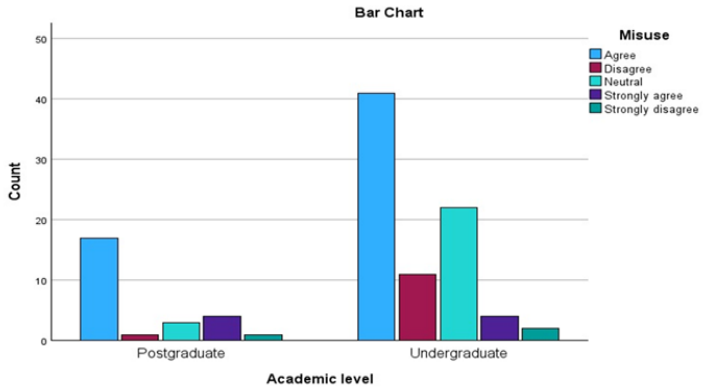

Fig. 1. Relationship Between Academic Level and Misuse of Facial Recognition Technology (FRT)

The figure illustrated that undergraduate students exhibited greater concerns regarding the misuse of FRT compared to their postgraduate peers. Among the surveyed group, forty-one undergraduates (70.7%) believed that FRT usage involved misuse, while only seventeen postgraduates (54.8%) shared this perspective. Furthermore, a notable number of undergraduates (22) expressed uncertainty about misuse, contrasting with just three postgraduates who felt similarly. These findings underscore that undergraduate students possess heightened concerns about privacy and the potential risks associated with FRT, attributable to their inexperience or limited exposure to such technologies. Existing literature suggests that less experienced individuals typically demonstrate greater distrust towards data handling practices (Smith and Miller, 2021). The CPM theory supports this finding, indicating that a lack of

control over personal information may lead students to perceive higher risks. Institutions need to intensify their efforts in addressing these concerns to foster a more trusting environment surrounding data management.

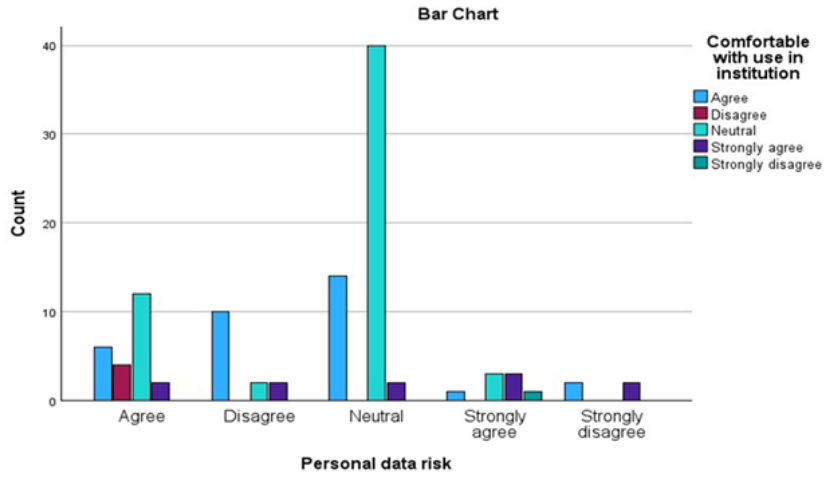

Fig. 2. Relationship Between Personal Data Risk and Comfort with Using FRT

This figure demonstrated that students perceiving a considerable risk to their personal data tended to feel less at ease with FRT. Among those who identified significant data risks, a larger proportion selected "Neutral" (12) compared to those who "Agreed" (6) with being comfortable using FRT. Conversely, students with minimal concerns about personal data risks expressed more comfort with technology, with 1 Strongly Agree and 2 Agree. These results aligned with the CPM theory, indicating that heightened concerns over data privacy correlate with increased discomfort towards data-collection technologies. The findings suggest that addressing privacy issues and ensuring robust protective measures can enhance acceptance of FRT. Research by Harper, Ellis, and Tucker (2021) highlights that user acceptance of surveillance technology improves when there's a perceived commitment to privacy protection and transparency.

Tab. 2. Relationship Between Field of Study and Perceptions of Effectiveness of Current Safeguards

Field of Study vs Privacy safeguards in institution Crosstabulation

Count

		Privacy safeguards in institution					
		Agree	Disagree	Neutral	Strongly agree	Strongly disagree	Total
Field of Study	Commerce	1	1	5	2	0	9
	Education	2	0	10	0	0	12
	Humanities	3	0	12	0	0	15
	Law	13	0	2	0	0	15
	Science & Technology	17	6	27	3	2	55
Total		36	7	56	5	2	106

The data from Table 2 revealed that students in Science and Technology fields were more likely to question the effectiveness of existing privacy safeguards compared to students in other disciplines. Among the thirty-eight students from Science and Technology, six expressed disagreements with the effectiveness of these measures, while students from Humanities and Education demonstrated more neutral sentiment towards privacy protections. This indicates that students better versed in technology and data handling might exhibit heightened awareness and expectations regarding privacy measures. These findings aligned with the CPM theory, highlighting the importance of transparency and control over personal information. It underscores the need for institutions to actively engage with students from various fields to better address diverse privacy concerns and tailor communication strategies accordingly.

Tab. 3. Relationship Between Data Collection Comfortability and the Need for Institutional Measures

Data Collection comfortability vs Robust measures Crosstabulation

Count

		Robust measures					
		Agree	Disagree	Neutral	Strongly agree	Strongly disagree	Total
Data Collection comfortability	Agree	24	0	1	7	0	32
	Disagree	7	1	3	2	0	13
	Neutral	33	0	4	10	1	48
	Strongly agree	0	0	0	5	0	5
	Strongly disagree	2	1	3	2	0	8
Total		66	2	11	26	1	106

Table 3 displayed a trend where students who felt comfortable with data collection supported the necessity for strong privacy measures—24 agreed and seven strongly agreed. In contrast, those uncomfortable with data collection were less likely to advocate for heightened protections, reflecting a disconnect between data comfort and perceived efficacy of safeguards. These findings aligned with the CPM theory, suggesting that comfort with data management influences support for robust privacy protections. Studies indicate that trust in data handling practices fosters a propensity for advocating for improved safeguards (Bhadouria, 2023). Conversely, discomfort with data collection could result in reduced advocacy for protective measures, as individuals may harbor skepticism regarding current practices.

Tab. 4. Descriptive Statistics for Privacy Concerns and Safeguards

Statistics

		Privacy Implications Concern	Misuse	Data Collection comfortability	Personal data risk	Privacy safeguardsat institution	Sufficient information	Current safeguards	Feel informed
N	Valid	106	106	106	106	106	106	106	106
	Missing	0	0	0	0	0	0	0	0
Mean		2.55	1.92	2.47	2.57	2.34	2.88	2.65	3.08
Median		3.00	1.00	3.00	3.00	3.00	2.00	3.00	3.00
Mode		3	1	3	3	3	2	3	2
Std. Deviation		1.088	1.160	1.189	1.042	1.059	1.343	.851	1.405

The data presented in Table 4 revealed a neutral to slightly concerned disposition among students regarding privacy issues, with an average score of 2.55. Responses concerning the perceived misuse of facial recognition technology averaged 1.92, illustrating disagreement with the notion of misuse. Additionally, students felt slightly uncomfortable with data collection practices, scoring an average of 2.47, and expressed modest skepticism towards the effectiveness of privacy protections (average score 2.34). The mixed sentiments surrounding privacy concerns reflect a broader societal ambivalence towards surveillance technologies. Citing research by Katsanis et al. and Roundtree (2023), these results highlight a need for improved clarity and efficacy in privacy protections, particularly in educational settings. The call for better transparency and robust policies echoes Wu's (2024) suggestions for enhanced ethical guidelines in privacy management. Overall, the study indicates a combination of neutrality and unease regarding existing privacy measures.

Tab. 5. Descriptive Statistics for Various Aspects of Facial Recognition Technology (FRT)

Statistics

		Student decision making	Robust measures	Strict policy development	Student consent	Comfortable with use in institution	Data responsibility	Benefits vs risks
N	Valid	106	106	106	106	106	106	106
	Missing	0	0	0	0	0	0	0
Mean		2.50	2.00	2.22	1.89	2.46	2.31	2.39
Median		2.50	1.00	1.00	1.00	3.00	3.00	3.00
Mode		1	1	1	1	3	3	3
Std. Deviation		1.475	1.345	1.387	.969	1.071	1.072	1.092

Table 5 displayed neutral attitudes toward FRT, with an average score of 2.50. Students felt moderately uncomfortable regarding data collection (average score of 2.46) while expressing skepticism regarding

policy strictness (2.22). The concerns surrounding consent and responsibility for data handling also reflected a mix of unease and neutrality. These results highlight the necessity for improved institutional policies and communication strategies. Recent studies corroborate the findings, reinforcing the need for transparency and effective privacy practices (Wu, 2024; Fu and Lyu, 2022). The CPM theory serves as a practical framework for managing privacy in educational contexts, emphasizing the establishment of strong protocols governing data management and usage (Petronio and Hernandez, 2019).

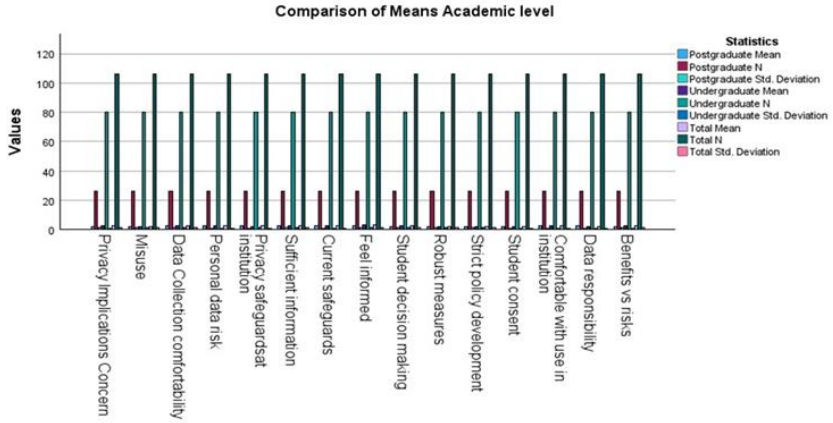

Fig. 4. Comparison of Means by Academic Level

Undergraduate students were found to have higher privacy concern scores (2.77) than postgraduate students (1.85). Despite shared worries regarding data misuse, postgraduate students demonstrated greater comfort with data collection practices. Additionally, postgraduate students reported slightly higher anxiety regarding personal data risks. These findings reaffirm the link between educational level and privacy perceptions, indicating that individuals with higher educational attainment may possess a better understanding of data management practices (Wang et al., 2020). The CPM theory supports the notion that perceived control of information contributes to overall comfort and trust in privacy management, suggesting that institutions should focus on enhancing the privacy literacy of undergraduate students.

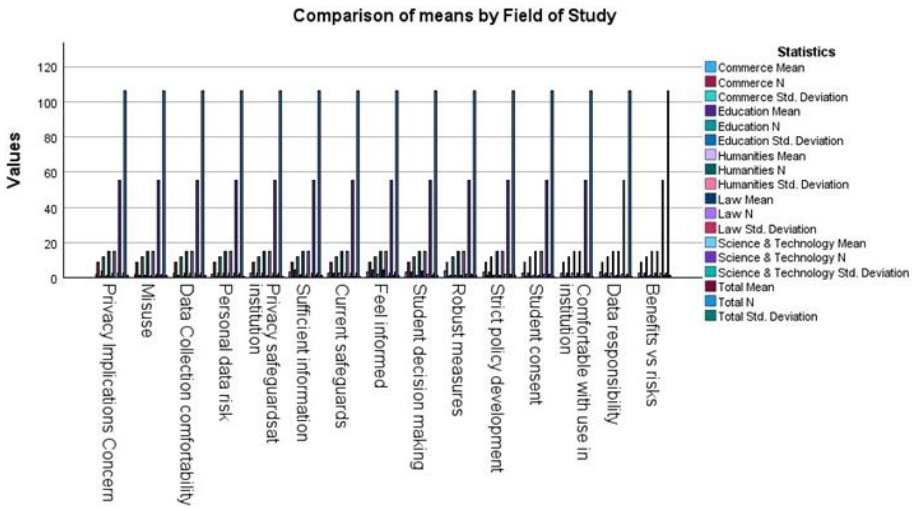

Fig. 5. Comparison of Means by Field of Study

Students studying Education expressed the highest privacy concerns (mean = 3.58), while Humanities students were the least concerned (mean = 1.27). Variations in perceptions of data risks, comfort with technology, and views on institutional privacy protections were observed across different academic disciplines. These divergences stem from differing levels of exposure to technology and ethical

considerations inherent in various fields. Education students, dealing with sensitive information regularly, may have heightened awareness of privacy issues, while Humanities students might be less engaged with privacy-related topics (Kumi-Yeboah et al., 2023). The CPM theory asserts the importance of crafting privacy policies that accommodate distinct academic perspectives to improve transparency and trust. Institutions should consider these differences when creating and communicating privacy measures tailored to meet the unique needs of each academic discipline.

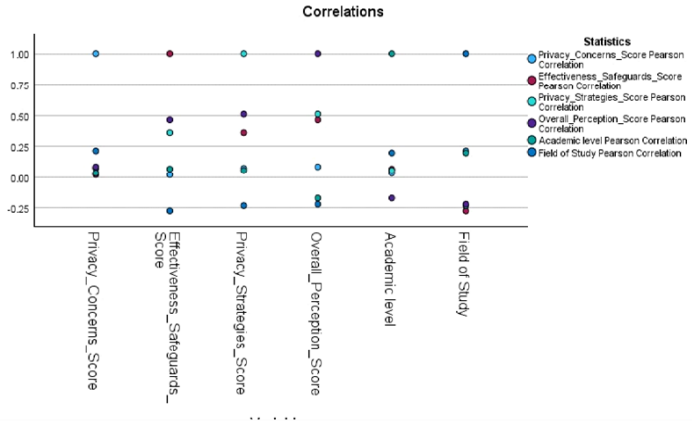

Fig. 6. Correlation Between Privacy-Related Scores and Academic Variables

The analysis revealed a significant positive correlation between perceptions of safeguard effectiveness and overall privacy sentiments. In contrast, a notable negative relationship existed between the field of study and perceptions of privacy strategies and safeguard effectiveness, indicating critical viewpoints among certain disciplines. These findings aligned with the principles of CPM theory, which posits that effective privacy management correlates positively with satisfaction regarding privacy practices. The strong connection between good privacy protections and positive opinions about privacy shows that establishing strong privacy practices can lead to greater satisfaction with data handling. The negative correlations related to the field of study suggest that different academic disciplines can influence individuals' perceptions of privacy in varied ways. This aligns with prior research indicating that individuals from technology-intensive fields may maintain higher scrutiny of privacy measures (Biselli & Reuter, 2021). Further investigation may be warranted to explore the factors influencing diverging views on privacy across academic programs, as this insight could inform more effective privacy management strategies tailored to specific disciplines.

6. CONCLUSION

The research revealed significant concerns about privacy, particularly regarding data collection, storage, and usage, with students often feeling that the institution does not provide adequate information. Those with limited knowledge of FRT are more likely to worry about privacy issues. The study emphasizes the need for organizations to prioritize transparency in discussions about FRT, suggesting that clear communication about data usage can alleviate privacy anxieties and that student involvement in privacy policy discussions is essential for building trust. While the research addresses privacy concerns related to FRT, its focus on a single institution and potential sample bias limit the generalizability of findings. Future studies should expand to different educational institutions and cultural contexts to better understand varied privacy concerns, as well as conduct long-term investigations tracking changes in attitudes toward privacy as FRT usage increases. Overall, the study enhances understanding of FRT in South African educational settings and highlights the importance of considering students' privacy perspectives, aligning with the Communication Privacy Management (CPM) theory by underscoring the need for control over personal information and transparency in data usage to foster a privacy-conscious environment.

REFERENCES

1. Andrejevic, M., and N. Selwyn. 2019. "Facial Recognition Technology in Schools: Critical Questions and Concerns." *Learning, Media and Technology* 45 (2): 1–14. https://doi.org/10.1080/17439884.2020.1686014.
2. Aswad, J., and J. Marx Gómez. 2021. "Data Ownership: A Survey." *Information* 12 (11): 465. https://doi.org/10.3390/info12110465.
3. Bhadouria, B. 2023. "Overcoming Barriers and Promoting Responsible AI Development: Artificial Intelligence Ethical Considerations." *International Journal of Scientific and Research Publications.* https://doi.org/10.29322/ijsrp.13.09.2023.p14105.
4. Biselli, T., and C. Reuter. 2021. "On the Relationship Between IT Privacy and Security Behavior: A Survey Among German Private Users." In *Lecture Notes in Information Systems and Organisation*, 388–404. https://doi.org/10.1007/978-3-030-86797-3_26.
5. Fu, H., and Y. Lyu. 2022. "Facial Recognition Interaction in a University Setting: Impression, Reaction, and Decision-Making." In *Advances in Intelligent Systems and Computing*, 329–343. https://doi.org/10.1007/978-3-030-96957-8_29.
6. Gies, W., J. Overby, N. Saraceno, J. Frome, E. York, and A. Salman. 2020. "Restricting Data Sharing and Collection of Facial Recognition Data by the Consent of the User: A Systems Analysis." *IEEE Xplore.* https://doi.org/10.1109/SIEDS49339.2020.9106661.
7. Harper, D.J., D. Ellis, and I. Tucker. 2022. "Covert Aspects of Surveillance and the Ethical Issues They Raise." In *Ethical Issues in Covert, Security and Surveillance Research Advances in Research Ethics and Integrity*, 177–197.
8. Kharb, L., and D. Chahal. 2023. "Privacy Threats in Facial Recognition-Based Identity Verification." *International Journal of Advanced Research in Science, Communication and Technology*, 569–572. https://doi.org/10.48175/ijarsct-11686.
9. Knijnenburg, B.P., X. Page, P. Wisniewski, H.R. Lipford, N. Proferes, and J. Romano, eds. 2022. *Modern Socio-Technical Perspectives on Privacy*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-82786-1.
10. Kostka, G., L. Steinacker, and M. Meckel. 2020. "Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US." Germany, the UK and the US (February 10, 2020).
11. Lehmuskallio, A., and A. Lampinen. 2019. "Material Mediations Complicate Communication Privacy Management: The Case of Wilma in Finnish High Schools." *International Journal of Communication* 13: 19.
12. Meden, B., P. Rot, P. Terhorst, N. Damer, A. Kuijper, W. J. Scheirer, A. Ross, P. Peer, and V. Struc. 2021. "Privacy–Enhancing Face Biometrics: A Comprehensive Survey." *IEEE Transactions on Information Forensics and Security* 16: 4147–4183. https://doi.org/10.1109/tifs.2021.3096024.
13. Meden, B., M. Gonzalez-Hernandez, P. Peer, and V. Štruc. 2023. "Face Deidentification with Controllable Privacy Protection." *Image and Vision Computing* 134: 104678.
14. McClellan, E. 2020. "Facial Recognition Technology: Balancing the Benefits and Concerns." *Journal of Business and Technology Law* 15 (2): 363.
15. Mishra, A., S. S. Dash, and S. Tiwari. 2023. "Unlocking the Magic of Facial Recognition: Empowering Security and Emotions with SVM." *Journal of Data Acquisition and Processing* 38 (2): 2402.
16. Nesterova, I. 2020. "Mass Data Gathering and Surveillance: The Fight Against Facial Recognition Technology in the Globalized World." *SHS Web of Conferences* 74: 03006. https://doi.org/10.1051/shsconf/20207403006.
17. Petronio, S., and R. Hernandez. 2019. "Communication Privacy Management Theory." *Oxford Research Encyclopedia of Communication.* https://doi.org/10.1093/acrefore/9780190228613.013.373.
18. Richardson, R. 2022. "Facial Recognition in the Public Sector: The Policy Landscape." *German Marshall Fund of the United States.*
19. Roundtree, A. 2023. "User Expectations of Facial Recognition in Schools and Universities: Mixed Methods Analysis." *AHFE International.* https://doi.org/10.54941/ahfe1003959.
20. Sarabdeen, J. 2022. "Protection of the Rights of the Individual When Using Facial Recognition Technology." *Heliyon* 8 (3): e09086. https://doi.org/10.1016/j.heliyon.2022.e09086.
21. Sciencebox.uz. 2024. "Navigating the Ethical and Technological Landscape: The Future Trajectory of Facial Recognition Technology." [online].
22. Steinacker, L., M. Meckel, G. Kostka, and D. Borth. 2020. "Facial Recognition: A Cross-National Survey on Public Acceptance, Privacy, and Discrimination." [online]. https://arxiv.org/pdf/2008.07275.pdf.
23. Venditti, L., J. Fleming, and K. Kugelmeyer. 2019. "Algorithmic Surveillance: A Hidden Danger in Recognizing Faces." *Honors Theses.* https://digitalcommons.colby.edu/honorstheses/932/.

24. Wang, X., Y.C. Wu, M. Zhou, and H. Fu. 2024. "Beyond Surveillance: Privacy, Ethics, and Regulations in Face Recognition Technology." *Frontiers in Big Data* 7: 1337465.
25. Williamson, B., S. Bayne, and S. Shay. 2020. "The Datafication of Teaching in Higher Education: Critical Issues and Perspectives." *Teaching in Higher Education* 25 (4): 351–365. https://doi.org/10.1080/13562517.2020.1748811.
26. Wu, Y. 2024. "Facial Recognition Technology: College Students' Perspectives in China." *Journal of Research in Social Science and Humanities* 3 (1): 53–79. https://www.pioneerpublisher.com/jrssh/article/view/626/563 [Accessed March 22, 2024].
27. Zeng, Y., E. Lu, Y. Sun, and R. Tian. 2019. "Responsible Facial Recognition and Beyond." [online]. https://arxiv.org/pdf/1909.12935 [Accessed March 23, 2024].
28. Zhang, S., Y. Feng, and N. Sadeh. 2021. "Facial Recognition: Understanding Privacy Concerns and Attitudes Across Increasingly Diverse Deployment Scenarios," 243–262.