Privacy Awareness in NC State University

Ameya Chavan
North Carolina State University
Raleigh, United States
aachava2@ncsu.edu

Aditya Srivastava
North Carolina State University
Raleigh, United States
asrivas7@ncsu.edu

Sunandini Medisetti
North Carolina State University
Raleigh, United States
smedise@ncsu.edu

ABSTRACT

As we witness evolution of digital landscape, managing and protecting personal information has become of prime importance, particularly in higher education institutes. This study presents the complexities of how the university privacy policies affect its students' perceptions and attitudes towards privacy of their data.

KEYWORDS

Digital Privacy, Student Data Protection, Privacy Awareness, University Policies, Data Breach Risks, Trust in Education

1 INTRODUCTION AND MOTIVATION

In today's rapidly advancing digital landscape, the protection of personal data privacy has become a pressing concern, especially within academic institutions managing extensive student information. North Carolina State University (NCSU), a pioneer in technological advancements, has to deal with the challenge of safeguarding student data amid the ongoing digital transformation of educational processes.

In the backdrop of the digital era, which has brought unprecedented convenience but also heightened privacy concerns, universities like NC State, must prioritize protection of student data. This is not only essential for adhering to legal and ethical standards but also for nurturing a sense of security and trust among the student body.

Universities like NCSU collect a lot of sensitive information from it's students, including academic records, personal details, and financial data. Safeguarding this information is imperative, not just for compliance but also for fostering a secure environment where students feel a sense of trust.

However, as NCSU embraces digital transformation across educational delivery, research, and administrative functions, new challenges emerge. The integration of technology brings about a heightened risk of exposing student data to potential breaches. Striking a delicate balance between the advantages of technology and the necessity for stringent privacy measures becomes imperative, requiring constant vigilance.

The major challenge we faced is the lack of awareness among students regarding their privacy rights and existing university policies. This knowledge gap can lead to concerns, erode trust, and in extreme cases, result in potential privacy violations. Addressing this challenge isn't just a legal and ethical imperative; it is crucial for sustaining a positive and secure learning environment at NCSU.

The primary goal of this project is to delve into student concerns related to privacy policies at NCSU and evaluate the impact of existing university policies on students' perception of privacy. By gaining insights into these concerns and assessing policy effectiveness, the aim is to elevate privacy awareness among students and align university policies with the evolving needs of the digital age.

2 LITERATURE WORK

Privacy concerns within academic institutions have become a focal point in recent years, with educational data, including student records and assessments, becoming lucrative targets for cyber threats [1]. Smith et al. (2019) conducted a study underscoring the necessity for comprehensive privacy policies to safeguard student data in universities [1]. This research sheds light on the vulnerabilities that educational institutions face and emphasizes the need for robust policies to counteract potential cyber threats.

As universities navigate the terrain of digital transformation, the interplay between technology and privacy becomes increasingly intricate. Jones and Brown (2020) stress the significance of integrating privacy considerations into the design and implementation of digital technologies within educational settings [2]. This work highlights the evolving challenges in ensuring the privacy of student data amidst technological advancements in academia.

Understanding students' perceptions of privacy is critical for effective policy development. Johnson et al. (2021) conducted a survey revealing a significant percentage of students being unaware of their privacy rights and expressing concerns about the security of their personal data [3]. This study underscores the imperative of tailoring privacy policies to align with the expectations and concerns of the student body.

The relationship between privacy policies and trust is explored by Anderson and Williams (2018) [4]. Their research emphasizes that transparent and well-communicated privacy policies positively influence trust among students. Clear communication is identified as a key factor in effective privacy management, emphasizing the need for educational institutions to foster trust through transparent privacy practices.

"The Evolving Landscape of Data Privacy in Higher Education" [8], a research initiative by EDUCAUSE in partnership with Huron, delves into how data privacy is managed in higher education. This comprehensive study examines recent privacy legislation, explores challenges arising during the COVID-19 pandemic, and uncovers the most significant hurdles and promising paths forward for data privacy in higher education. Surveys and interviews with privacy professionals and leaders from various institutions provide a nuanced understanding of the current state of data privacy management.

Privacy concerns during the COVID-19 pandemic, particularly in the context of remote learning and work, are addressed in research conducted by EDUCAUSE [5]. This study emphasizes the need for comprehensive privacy policies and resources in higher education institutions, recognizing the gap in understanding between students and administrative plans and policies regarding data use. It suggests

a pressing need for improved privacy awareness and education across the academic landscape.

The report "Privacy Considerations in Higher Education Online Learning" [9] by Chris Sadler, the Education Data and Privacy Fellow at New America's Open Technology Institute, explores the intersection of privacy issues and the rapid transition to online learning in higher education, particularly in response to the COVID-19 pandemic. The author delves into various aspects, including applicable laws such as FERPA, GLBA, CCPA, and GDPR, and discusses the implications of these regulations on data privacy in online education. The document examines the technologies commonly used in distance learning, such as Learning Management Systems, videoconferencing, online program management companies, remote proctoring, mobile applications, and predictive analytics. Additionally, it addresses concerns related to privacy policies, data minimization, and retention practices, emphasizing the need for institutions and ed tech providers to navigate the delicate balance between leveraging data for educational improvements and safeguarding student privacy.

As educational institutions increasingly rely on technology to facilitate online learning, the report highlights the growing significance of comprehensive privacy measures. It underscores the need for transparent policies, especially in light of the surge in remote proctoring tools, mobile applications, and predictive analytics, which intensify data collection. The author also discusses the potential risks associated with videoconferencing, emphasizing the importance of safeguarding student information, especially for vulnerable populations. The report provides a critical overview of the challenges and considerations surrounding privacy in higher education's digital landscape, advocating for thoughtful policies and practices to ensure the responsible use of student data in the evolving online learning environment.

In order to assess the current state of privacy awareness and perception at NCSU, a comprehensive survey will be conducted among students across diverse demographics. This survey will probe into students' awareness of privacy policies, concerns related to data security, and their overall perception of the effectiveness of existing university privacy measures. Through this, NCSU aims to tailor its privacy policies to better align with the expectations and concerns of its student community.

3 PROPOSED RESEARCH

Our comprehensive research project unfolds in four distinct stages, each playing a pivotal role in unraveling the complexities surrounding student data privacy at North Carolina State University (NCSU)

(1) **Preliminary Research**: To lay a robust foundation for the investigation, a comprehensive review of existing university privacy policies, legal requirements, and prevailing best practices in data protection was conducted. This has involved a meticulous examination of the intricacies of NCSU's privacy policy [6], scrutinizing not only its content but also its alignment with regional and national regulations governing data privacy.
(2) **Survey Development and Distribution**: The heart of this research lies in understanding the nuanced perspectives of the student body regarding privacy policies. To achieve this, a meticulously designed survey is crafted, encompassing a spectrum of questions related to student awareness, experiences, and perceptions of privacy within the university ecosystem. Demographic data has been collected to ensure that the survey captures the diverse range of perspectives within the student community. This includes factors such as age, gender, ethnicity, academic discipline, and year of study. By understanding the variations in responses across these demographics, the research aims to identify any disparities in awareness and concerns.

The visualizations provided in the survey analysis shed light on various aspects of students' perceptions and experiences related to privacy within the university context.

Age vs Awareness: The data suggests that older age groups tend to exhibit higher awareness of university privacy policies. This could imply that the university's outreach efforts are effectively reaching a broad demographic or that awareness naturally increases with age and experience. Understanding this correlation is crucial for refining communication strategies and ensuring that privacy information is disseminated effectively across different age groups.

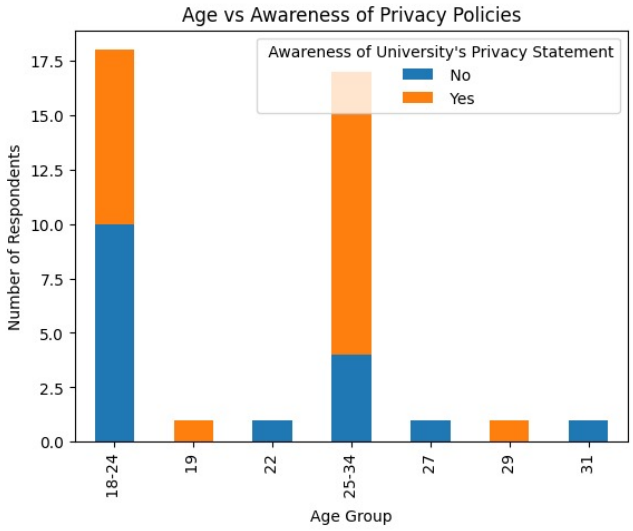

Figure 1: Age vs Awareness

Educational Status and Scam Recognition: The diverse levels of scam recognition confidence among graduates suggest that there may be varying degrees of awareness and preparedness across different educational statuses. Tailoring scam awareness education to accommodate the needs of students at various academic levels could enhance the effectiveness of such programs, contributing to a more informed and vigilant student body.

Data Breach Experience and 2FA Usage: The observed tendency for individuals with data breach experiences to be more likely to use two-factor authentication (2FA) indicates an increased awareness of security practices among this

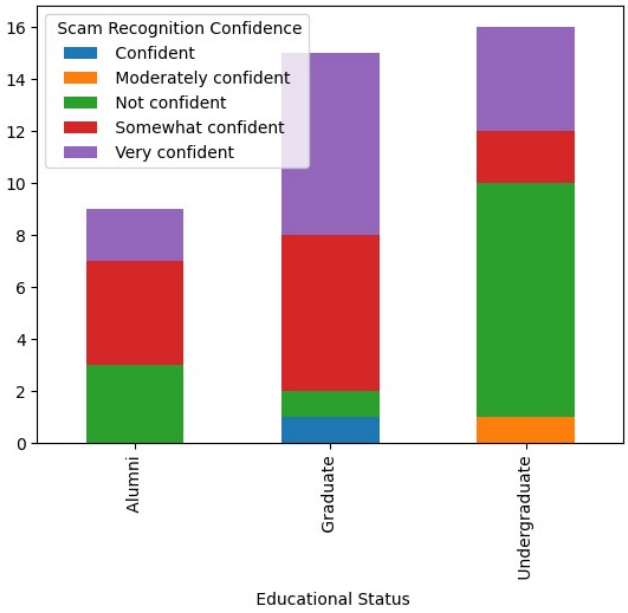

Figure 2: Educational Status and Scam Recognition

group. Leveraging this awareness to promote broader adoption of 2FA across all students could be an effective strategy in enhancing overall cybersecurity within the university.

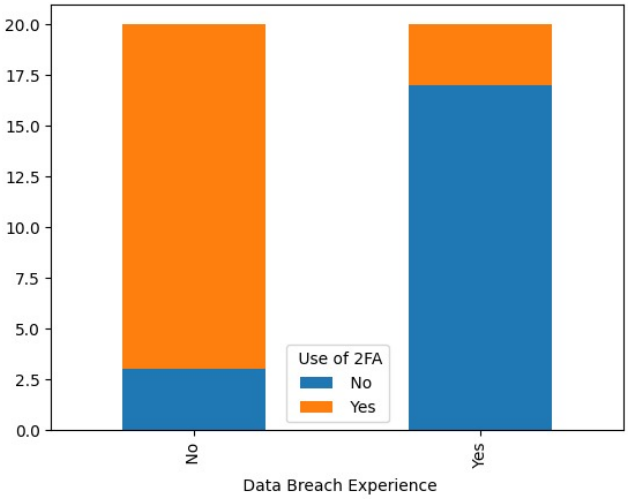

Figure 3: Data Breach Experience and 2FA Usage

Password Security and Data Use Confidence: The lack of a strong correlation between the use of strong passwords and confidence in understanding university data use suggests that students may perceive these as distinct aspects of cybersecurity. Addressing this perception gap through targeted educational initiatives can bridge the knowledge divide between practical security measures, like password management, and a comprehensive understanding of university data usage policies.

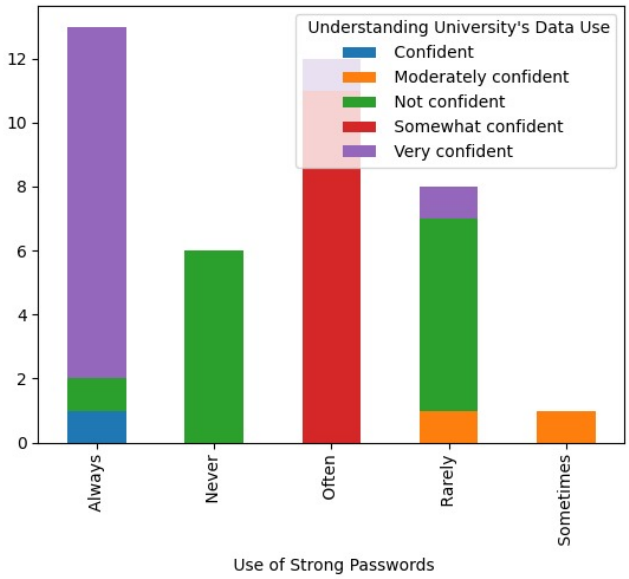

Figure 4: Password Security and Data Use Confidence

Gender and Data Breach Experience: The relatively equal distribution of data breach experiences across genders is a notable finding. This indicates that concerns related to data breaches are not exclusive to a particular gender, emphasizing the universality of the issue among students. Strategies and interventions aimed at preventing and mitigating data breaches should consider this gender-neutral trend, ensuring that security measures are inclusive and accessible to all.

Law Awareness and Data Misuse Actions: The influence of familiarity with data protection laws on the proactive actions students would take in response to unauthorized data sharing highlights the significance of legal literacy. Integrating information about relevant laws and regulations into privacy education initiatives can empower students to take informed and legally grounded steps in protecting their data.

Learning Methods and Data Use Understanding: Variations in the correlation between preferred learning methods and understanding the university's data use suggest that diverse educational approaches may be needed to effectively convey information about data usage policies. Customizing educational materials to align with different learning preferences, such as workshops, seminars, or online modules, can optimize the impact of privacy education initiatives.

Privacy Settings Review and Advocacy: The identified trend linking students who review their privacy settings with a higher likelihood of advocating for privacy practices underscores the importance of personal engagement in shaping broader privacy concerns. Encouraging students to actively manage their privacy settings can serve as a catalyst for fostering a culture of privacy advocacy within the university.

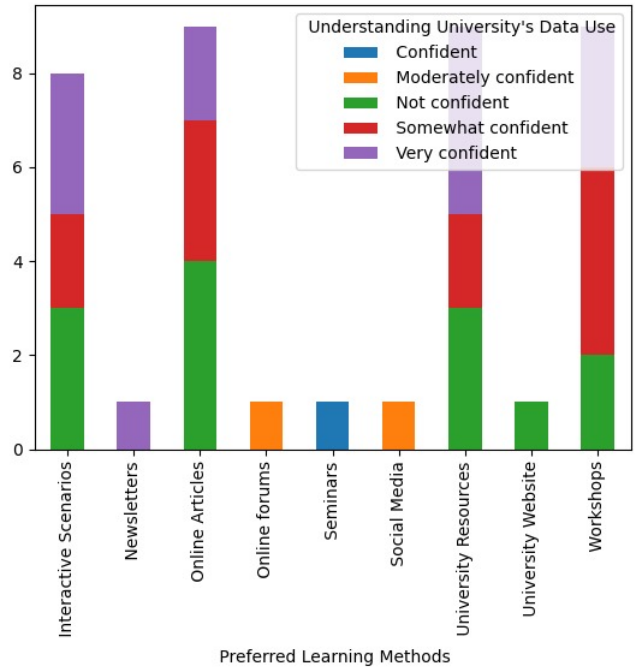

Figure 5: Preferred Learning Methods

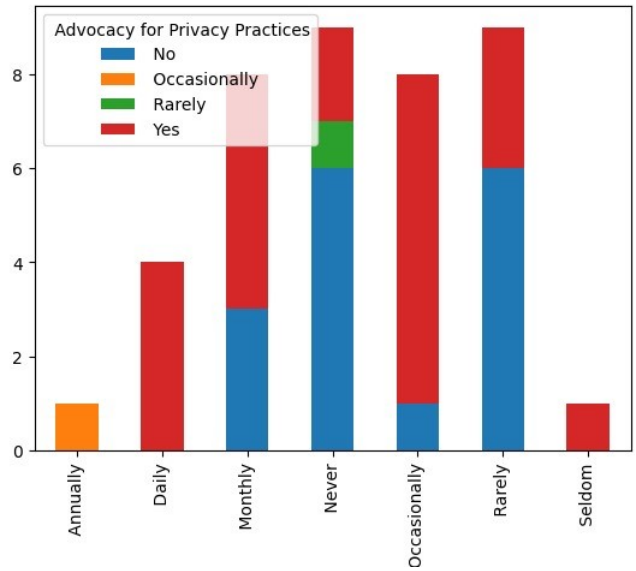

Figure 6: Privacy Settings Review and Advocacy

In summary, these visualizations provide valuable insights into the complex landscape of students' privacy perceptions and behaviors. Leveraging these findings can inform targeted strategies and interventions to enhance privacy awareness, encourage responsible data practices, and create a more secure and informed university community.

The survey has been crafted with a keen focus on user-friendliness and accessibility, recognizing the diverse backgrounds and technological proficiencies of the University population. Utilizing online platforms for survey distribution will not only streamline the data collection process but also enhance the reach, ensuring participation from a representative sample of the student body.

(3) **Data Analysis**: After the successful collection of data, we embarked on a meticulous process of collation and analysis. The primary objective was to unveil not only overarching trends but also to pinpoint specific concerns and identify potential areas of improvement within the university's privacy policy. To achieve a more nuanced understanding of student perspectives, the collected data was systematically categorized into themes.
In our analytical approach, each feature was assigned relevant weights [7] based on its influence on the dependent variable. This method allowed us to discern the significance of different aspects related to privacy. Moreover, we adopted an innovative strategy to distill these intricate data points into a user-friendly and comprehensible metric – the Privacy Perception Score (PPS). This score serves as a quantitative measure, providing a valuable tool for comparative analysis across diverse categories and demographics.
By assigning numerical values to privacy sentiments, the PPS not only facilitates a clearer understanding of the data but also enables a more structured and informed evaluation of the university's privacy landscape. This approach contributes to the depth and precision of our findings, ensuring a robust foundation for the subsequent stages of our research.
The formulated recommendations are a direct outcome of our in-depth data analysis, where we systematically categorized information into themes, assigned weights based on their influence, and devised the innovative Privacy Perception Score (PPS) to quantitatively measure privacy sentiments. These measures ensure that our recommendations are not only informed by overarching trends but also intricately tailored to the nuanced perspectives revealed in the data.

The aim is not merely to critique the current state of affairs but to collaboratively work towards enhancing student privacy awareness at NCSU and ensuring that university policies resonate with the expectations and rights of its diverse student community. The recommendations will be framed with a forward-looking perspective, considering the dynamic nature of both technology and privacy regulations.By fostering a deeper understanding of student concerns and perceptions, the ultimate goal is to lay the groundwork for a more robust, transparent, and privacy-conscious university ecosystem.

4 FINDINGS

To derive a quantifiable assessment of the privacy perception, the variables developed from the survey questions such as awareness, data breach experience, scam recognition confidence, secure password implementation practices, use of 2FA, review of privacy policies, and familiarity with law were assigned weights. Qualitative

Table 1: Survey Questions with Associate Weights

Question	Weight
Age	2
Gender	0
Educational Status	2.5
Data Breach Experience	-5
Scam Recognition Confidence	5
Use of Strong Passwords	2
Use of 2FA	2
Reviewing Social Media Privacy	2
Reviewing Smartphone Privacy	1
Checking App Privacy Policy	1
Familiarity with Data Protection Laws	2
Action if Data Shared Without Consent	3
Advocacy for Privacy Practices	3
Preferred Learning Methods	0
Awareness of University's Privacy Statement	2
Understanding University's Data Use	2

questions like preferred learning methods for better privacy perception were given a score of zero(0), and quantitative variables were scored based on the assumed they might have on the calculation of PPS. For example, someone with an experience of a data breach experience should have a lower PPS, hence the factor "Data Breach Experience" should be weighed negatively. Alternatively, factors like "Scam Recognition Confidence" indicate better understanding of privacy, and hence is weighed with a higher positive value. Based on these scores we performed the following steps to understand how different demographic variables affect the individual's PPS:

(1) Calculate the descriptive statistics of the data, that is, the mean, median, and mode of the PPS to understand the central tendency of privacy perception. Calculate the range, variance, and standard deviation to assess the spread of the scores.
(2) Further group the data by demographic categories and the perform comparisons of the average PPS across these groups. We used t-tests and ANOVA for calculating values of t-statistics and F-statistics to compare means and analyze if the differences have any statistical significance.
(3) We also perform correlation analysis between the PPS and other continuous variables (e.g., age) to find any linear relationships.
(4) As a part of future work, we can do regression analysis and predict PPS by the various factors we used to calculate the PPS.
(5) For visualization purposes we use boxplots and histograms to understand the distribution of PPS.
(6) Finally, in this section we try to present the findings with sufficient statistical evidence and visualizations.

In the above mentioned step (2) we perform analysis on the gathered data like t-test analysis between male and female groups, and also calculate the p-value. Further, we use ANOVA across groups based on Educational Status, namely F-statistic to understand variations between groups and among groups. Based on the results that we found in the above analysis we can state that:

(1) **Average PPS by Gender**: There is a noticeable trend between the mean value of Privacy Perception Scores(PPS) across genders. Groups like 'Prefer not to say' and 'Female' have higher average PPS, and are more aware and concerned towards privacy than 'Male' groups. This suggests that PPS vary significantly across gender groups.

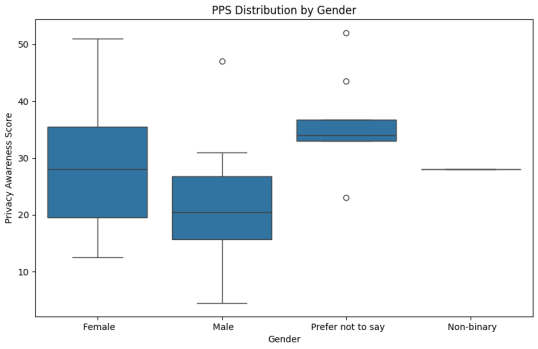

Figure 7: PPS Distribution by Gender

(2) **T-Test(Male vs. Female)**: However, when the t-test is performed over a confidence interval of 95% ($\alpha = 0.05$), we get a t-statistic value of -1.884 and a p-value of 0.069. This suggests that even though the p-value is close to the α level of 0.05, it is not statistically significant under the given threshold. This implies that even though there exists a trend between PPS values of male and female groups, it is not statistically significant. Mathematically, it means that is observed trend or difference is due to a random chance or small population size.
(3) **ANOVA(Analysis of variance formula) performed on Educational Status**: The F-statistic is calculated to be 6.574 and the p-value is 0.0036. This result suggests that there is significant among the three groups based on educational status, that is, Undergraduates, Graduates and Alumni. A P-value less than 0.05, indicates that the observed variance in PPS across different educational statuses is statistically significant and a higher F-stat value denotes a higher likelihood that these differences are due to differences among the groups and not within the groups.

Further, as mentioned in step (3) we performed correlation analysis between the statistically significant groups to further analyze their relationship with the privacy perception scores (PPS). Here we try to generation a correlation matrix [Table 2] between Undergraduate, Graduate and Alumni as compared to the PPS.

(1) **Alumni:** A negative correlation value of -0.158770 depicts a weak relationship, and suggests that alumni tend to have lower PPS compared to other groups. This highlights the point that Alumni are less concerned and affected by how university privacy policies change.

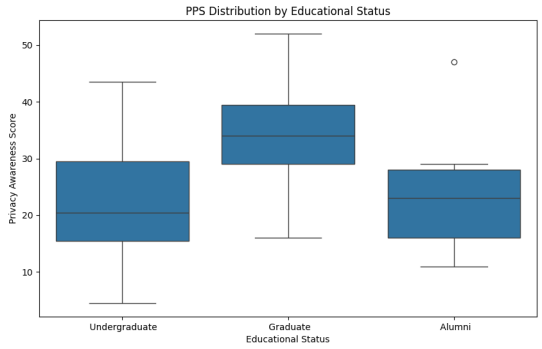

Figure 8: PPS Distribution by Educational Status

Educational Status	PPS
Undergraduate	-0.351353
Graduate	0.492493
Alumni	-0.158770

Table 2: Correlation Matrix: Educational Status vs PPS

(2) **Graduate:** This group has a moderate positive correlation value of 0.492493. This indicates that graduate students tend to have higher PPS, and have higher awareness and concerns about privacy.
(3) **Undergraduates:** Even undergraduates are seen to have lower awareness and concern about privacy. This is highlighted by the moderate negative correlation value of -0.351353.

5 CONCLUSIONS

The findings suggest that there is a strong correlation between a person's educational status and the privacy perception score.

(1) **Correlation between Education and PPS:** These correlations indicate that the higher median PPS among graduates, highlighting the importance of privacy related education throughout the academic journey.
(2) **Importance of Privacy Education:** This integration of privacy concepts can be pivotal in cultivating more informed and privacy conscious students. This is important as in today's digital age, personal information is continuously shared and exposed online.
(3) **Integrating Privacy Education in University Curricula:** NC State university can consider improving their curriculum to include privacy education not just at advanced education levels but starting from undergraduate courses. This can ensure that all students, irrespective of their stage in education, receive a good fundamental understanding of privacy concepts. This should be done with goal that students become more aware and responsible when it comes to handling matters of privacy.
(4) **Targeted Approaches for Diverse Student Populations:** These findings indicate that various student groups divided on different demographics have varying level of privacy awareness. For example, the male students and alumni have lower PPS. This helps us understand that there is need for universities to develop targeted strategies that handle the needs and awareness levels for these diverse groups. Specifically prepared approaches could be more effective in engaging these groups and improving their understanding of privacy issues.

6 FUTURE DIRECTIONS

Our project's trajectory extends into the realm of advanced analytics through Feature Importance Analysis, leveraging machine learning algorithms. This phase aims to unravel the significance of each feature in predicting the Privacy Perception Scores (PPS). By employing sophisticated algorithms, we anticipate gaining profound insights into the factors that contribute most significantly to shaping privacy perceptions within the university community.

The analysis will involve the application of machine learning models capable of discerning the weight and impact of different features on the overall Privacy Perception Scores. Regression models, such as Random Forests or Gradient Boosting, will be considered for their ability to handle complex relationships within the data.

Upon completion of the Feature Importance Analysis, we envisage a comprehensive understanding of the hierarchy of factors influencing privacy perceptions among students. This insight will not only highlight the most influential elements but also shed light on potential correlations and interactions between different features.The insights derived from the Feature Importance Analysis will be instrumental in shaping targeted policy adjustments. By identifying the most influential factors, the university can tailor its privacy policies to address specific concerns and enhance privacy perceptions effectively. This proactive approach ensures that policy changes are not arbitrary but rooted in data-driven decision-making

Understanding the key factors influencing privacy perceptions allows for a strategic approach to communication. The results of this analysis will guide the development of targeted communication strategies, ensuring that privacy-related information is effectively communicated to the student body. By focusing on the factors identified as crucial, the university can enhance transparency and trust in its privacy initiatives.

The integration of Feature Importance Analysis into our project signifies a commitment to a holistic approach in improving privacy measures. Rather than a one-size-fits-all strategy, this analysis allows for a nuanced and tailored response, aligning policies and communication with the specific concerns and expectations of the diverse student population.

In essence, the Feature Importance Analysis represents a pivotal step towards not only understanding the dynamics of privacy perceptions but also actively leveraging these insights to enhance privacy measures and communication within the university ecosystem. This forward-looking approach ensures that our project contributes not only to academic research but also to tangible improvements in the privacy experience of students at North Carolina State University.

7 TEAM CONTRIBUTION

All the members of the team were involved in all parts of the project. However, the following parts were led majory by -

- Literature Review : Aditya
- Preliminary Research: Sunandini
- Survey Design and Response Validation : Ameya
- Privacy Awareness Score calculation : Aditya
- Data Analysis and Visualizations : Ameya
- Presentation : Sunandini
- Project Report : All team members

REFERENCES

[1] A. Smith *et al.*, "Protecting Student Data Privacy in Higher Education: An Overview of Current Practices," 2019.
[2] M. Jones and C. Brown, "Digital Transformation in Higher Education: A Case Study of Privacy Challenges and Opportunities," 2020.
[3] L. Johnson *et al.*, "Student Perspectives on Privacy in Higher Education: A Survey Study," 2021.
[4] R. Anderson and P. Williams, "Building Trust in Digital Education: A Privacy-Centered Approach," 2018.
[5] EDUCAUSE, "Key Findings on Privacy in Higher Education," https://er.educause.edu/blogs/2020/12/key-findings-on-privacy-in-higher-education.
[6] North Carolina State University, "Privacy at NC State," https://www.ncsu.edu/privacy/.
[7] Analytics Vidhya, "Improve Class Imbalance: Class Weights," https://www.analyticsvidhya.com/blog/2020/10/improve-class-imbalance-class-weights/.
[8] EDUCAUSE, "The Evolving Landscape of Data Privacy in Higher Education," https://library.educause.edu/resources/2020/11/the-evolving-landscape-of-data-privacy-in-higher-education.
[9] Chris Sadler, "Privacy Considerations in Higher Education Online Learning," https://d1y8sb8igg2f8e.cloudfront.net/documents/Privacy_Considerations_in_Higher_Education_Online_Learning_2020-10-22_154612_JNk73qJ.pdf.
[10] https://www.iiisci.org/journal/pdv/sci/pdfs/IP099LL20.pdf
[11] GitHub - Privacy Awareness, https://github.ncsu.edu/asrivas7/privacy_awareness.