ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

CONVENIENCE VS. CONSENT: EXPLORING THE PERSONALISATION-PRIVACY PARADOX IN THE DAILY DIGITAL HABITS OF COLLEGE STUDENTS

*** *Ameer Pathan, **Sabrin Shaikh, ***Shwetanksha Yadav & ****Dr. Madhu Shukrey***

** Assitant Professor , ** UG Students, *** UG Students & **** Assitant Professor, Department of IT/CS, B. K. Birla College, Kalyan, Mumbai, India*

Abstract:

This study examines the personalisation–privacy paradox in the daily digital habits of college students, focusing on the relationship between privacy concern, perceived benefits of personalisation, digital literacy, and actual privacy protection behaviour. Using a mixed-method approach, primary data from 75 respondents were analysed through correlation, regression, t-test, and Friedman tests, supported by qualitative case review. The findings reveal no significant relationship between privacy concern and protection behaviour, but confirm a significant gap between expressed concern and actual actions. Digital literacy plays a key role in how well students understand informed consent. The study shows that, even as urban college students become more aware of privacy issues, they often stick to convenient habits online.

Key Words: *Personalisation–Privacy Paradox, Privacy Concern, Privacy Protection Behaviour, Digital Literacy, Informed Consent, Online Privacy*

Introduction

College students' digital lives are deeply affected by personalisation. Digital platforms adapt Instagram feeds, Netflix recommendations, targeted ads and location- based services to suit individual interests, more seamless and appealing digital experiences. However, this convenience often comes with the ongoing transfer of personal data sometimes disclosed knowingly, but often without users fully realizing it. Even with growing privacy concerns, students continue depend on these platforms, highlighting the personalisation–privacy paradox.

In fast-growing urban regions like the Mumbai Metropolitan Region (MMRDA), digital tools have become part of everyday life rather than optional conveniences. Fast paced digital use encourages quick consent and minimum examination of privacy policy. Although students are technically skilled, varying levels of digital literacy shape how effectively they understand, manage and protect their personal data.

Statement of the problem:

Digital platforms have become a regular part of college students' daily lives, supporting their studies, financial transaction, social interactions, and entertainment. Personalisation has made these platforms quicker and easier to use, but it also requires regular sharing of personal information. Although many students say they care about

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

privacy, their everyday online behaviour such as accepting cookies or granting app permissions often do not match these concerns. Frequent use of digital platforms also does not always mean better understanding, as long and complicated privacy policies encourage users to give consent without reading them carefully, reducing awareness of how personal data is collected and used. This issue is particularly noticeable in the Mumbai Metropolitan Region (MMRDA), where digital usage is high but digital literacy levels differ. As a result, even when students try to protect their privacy, they often continue risky practices like oversharing or using unsafe networks, revealing a clear gap between privacy concerns and daily online behaviour.

Significance of study:

In today's data-driven world, personalisation is commonly viewed as an advantage. College students in cities like the Mumbai Metropolitan Region (MMRDA) frequently use digital platforms for education, communication, transactions, entertainment and job skill. Yet, few studies investigate how well they understand privacy, consent and data use. This study explores the personalisation–privacy paradox, analysing how digital literacy supports informed consent and responsible online behaviour, offering valuable support for educators, policymakers and platform designers to promote safer, clearer digital practices.

Limitations of the study:

The study relies on self-reported questionnaire data, which may be influenced by social desirability response tendency and inaccurate recall of digital behaviour.

The cross-sectional design limits observation of changes in attitudes over time. Although it is supported by secondary sources, the absence of in-depth interviews or focus groups restricts deeper psychological insight.

Time constraints limited prolonged data collection and behavioural tracking. Additionally, the geographically restricted sample may affect broader applicability.

Rapid technological changes may also influence the long-term relevance of the findings.

Objectives of the study

The objectives of the study are as follows:

1. To examine the personalisation–privacy paradox among college students in their daily digital habits.
2. To assess the impact of digital literacy on informed consent decisions.
3. To analyse the relationship between privacy concern levels, perceived benefits of personalisation, and privacy protection behaviour among college students.

Hypothesis of the study:

Null Hypothesis (H01)

There is no significant relationship between privacy concern level, perceived benefits of personalisation, and privacy protection behaviour among college students.

Alternative Hypothesis (H11)

There is a significant relationship between privacy concern level, perceived benefits of personalisation, and privacy protection behaviour among college students.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Null Hypothesis (H02)

There is no significant impact of digital literacy on informed consent among college students.

Alternative Hypothesis (H12)

There is a significant impact of digital literacy on informed consent among college students.

Null Hypothesis (H03)

There is no significant gap between privacy concern and actual online behaviour among college students.

Alternative Hypothesis (H13)

There is a significant gap between privacy concern and actual online behaviour among college students.

Review of literature:

1. **Personalisation–Privacy Paradox among College Students**

   Several studies highlight users' increasing reliance on personalized digital services and its impact on privacy. Alessandro Acquisti, Laura Brandimarte, and George Loewenstein (2015) found that although individuals claim to value privacy, they often sacrifice it for immediate benefits like convenience and personalisation demonstrating the privacy paradox, where expressed concerns do not match actual disclosure behaviour. (Acquisti, 2015)

   Sabine Trepte et al. (2017) found that users share personal data when perceived benefits exceed risks. Among students, personalized recommendations, targeted ads, and customized content boost engagement despite ongoing concerns about privacy and potential data misuse. (al., 2017)

2. **Digital Literacy and Informed Consent Decisions**

   Livingstone, van Couvering and Thumim (2018) emphasized that young users frequently accept terms and conditions without reading or understanding them, primarily due to complex language, time constraints and cognitive overload. This weakens informed consent and increases vulnerability to privacy risks. (Livingstone, 2018)

   The findings indicate that digital literacy programmes conducted by institutional libraries significantly improve the digital literacy level of management students by strengthening their ability to access and use ICT-based information resources effectively. (Baban K. More, 2020)

   The findings indicate that effective explanation and simplified presentation of consent forms significantly improve participants' understanding, ensuring informed and voluntary research participation. (Tara van Dijk, 2016)

3. **Gap between Privacy Concern and Actual Online Behaviour**

   Barth and de Jong (2017) demonstrated that risky online behaviours', such as weak password usage, excessive sharing and unverified app permissions, persist despite high privacy awareness. This indicates a strong awareness–action gap. (jong, 2017)

   The findings indicate that although privacy settings are available, users often underutilize them due to limited awareness and difficulties in understanding privacy control mechanisms. (Vashistha, 2018)

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Research Gap Summary:

Existing research shows limited focus on the personalisation–privacy paradox among Indian college students, lacks strong empirical links between digital literacy and informed consent, and insufficiently examines the gap between privacy concerns and actual online behaviour. This study addresses these interconnected gaps.

Research methodology:

The study follows a descriptive and analytical approach using a mixed-method research design. The descriptive aspect helps in clearly understanding current digital behaviour patterns, privacy concerns, use of personalized services, and consent practices among college students. The analytical aspect examines relationships between key variables such as personalisation, privacy concern, digital literacy, and actual online behaviour, allowing hypothesis testing and identification of gaps between attitudes and actions.

The quantitative method is used to measure relationships through structured numerical data, while qualitative insights are drawn from secondary data analysis to better understand students' perceptions and reasoning. Together, this approach provides a balanced and deeper understanding of the personalisation–privacy paradox.

Data analysis and interpretation:

1. ***Introduction***

   This chapter analyses both primary and secondary data. Primary data from 75 college students were collected through a structured questionnaire. Using IBM SPSS Statistics, Pearson correlation examined relationships among Privacy Concern, Perceived Benefits of Personalisation, and Privacy Protection Behaviour; multiple regression assessed Digital Literacy's impact on Informed Consent Understanding; a t-test analysed differences between Privacy Concern and Actual Online Behaviour; and Friedman's K-Sample Test evaluated ranking-based questions. The secondary data section includes a qualitative data table.

2. ***Demographic Profile of Respondent***

   The study included 75 college-going students. Respondents belonged to different age groups ranging from 18 years and above. The questionnaire also captured average daily internet usage.

Table 1 : Age Group Distribution

(Frequency and Percentage)

Age Group	Frequency (Count)	Percentage (%)
18–19 years	28	37.3
19–20 years	32	42.7
20–21 years	12	16.0
21 years and above	3	4.0
Total	**75**	**100**

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a)

Jan – Feb 2026

Original Research Article

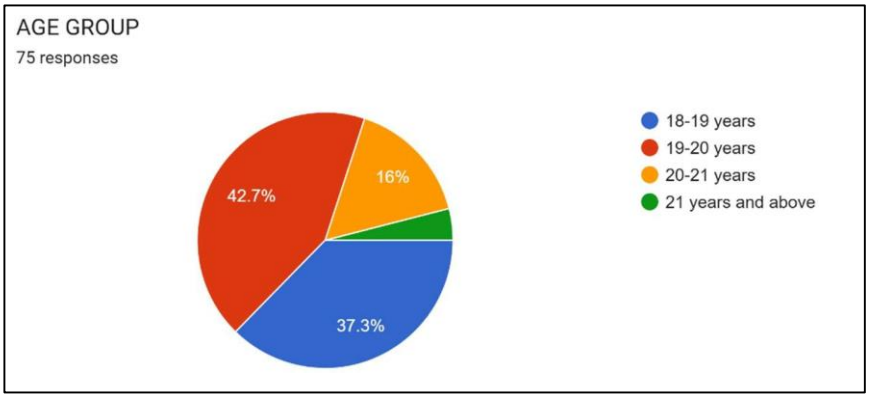


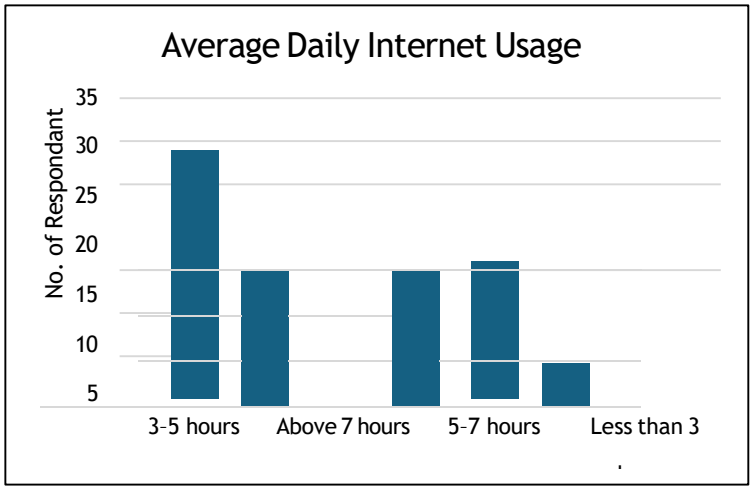
Figure 1: Age Group Distribution of respondents'

Table 2 Average Daily Internet Usage (Frequency and Percentage)

Average Daily Internet Usage	Frequency (Count)	Percentage (%)
3–5 hours	29	38.70%
Above 7 hours	20	26.70%
5–7 hours	16	21.30%
Less than 3 hours	10	13.30%
Total	**75**	**100%**

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

Figure 2 Figure 2 Daily Internet usage pattern of the respondents'



(Source: Primary data collected through questionnaire and analysed by SPSS tools)

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

a. Analysis of the Personalisation–Privacy Paradox

To examine the personalisation–privacy paradox among college students in their daily digital habits.

Correlation Analysis

Three key variables were analysed:

i. Privacy Concern
ii. Perceived Benefits of Personalisation
iii. Privacy Protection Behaviour

Pearson correlation analysis was conducted to examine the relationship among these variables.

Table 3 Pearson Correlation Matrix (Objective 1 Variables)

Correlations				
		PC	PB	PPB
Privacy Concern	Pearson Correlation	1	.009	.034
	Sig. (2-tailed)		.938	.772
	N	75	75	75
Perceived Benefits	Pearson Correlation	.009	1	.222
	Sig. (2-tailed)	.938		.056
	N	75	75	75
Privacy Protection Behavior	Pearson Correlation	.034	.222	1
	Sig. (2-tailed)	.772	.056	
	N	75	75	75

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

The results show:

iv. Privacy Concern and Perceived Benefits ($r = 0.009$, $p = 0.938$)
v. Privacy Concern and Privacy Protection Behaviour ($r = 0.034$, $p = 0.772$)
vi. Perceived Benefits and Privacy Protection Behaviour ($r = 0.222$, $p = 0.056$)

All p-values are greater than 0.05, indicating that none of the relationships are statistically significant.

Hypothesis Testing:

H_{01}: There is **no significant relationship** between privacy concern, perceived benefits, and privacy protection behaviour.

H_{11}: **There is a significant relationship** between these variables.

Since **all p-values exceed 0.05**, the **null hypothesis is accepted** and the alternative hypothesis is rejected.

Interpretation:

The findings suggest that although students' express privacy concerns and acknowledge the benefits of personalisation, these factors do not significantly influence their privacy protection behaviour. Therefore, based on correlation analysis, a strong personalisation–privacy paradox is not statistically established in this sample.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Ranking Analysis (Friedman Test)

Two ranking questions were analysed under Objective 1. Platforms Perceived to Collect the Most Data

Table 4 Mean Ranks – Data Collection Platforms

Ranks	
	Mean Rank
O1_Q1_INSTA	1.70
O1_Q1_GOOGLE	2.18
O1_Q1_AMAZON	2.91
O1_Q1_SNAPCHAT	3.21

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

Instagram/Facebook received the lowest mean rank (1.70), indicating that students perceive it as the platform collecting the most data. This was followed by Google/YouTube (2.18), Amazon (2.91), and Snapchat (3.21).

Benefits of Personalisation:

Table 5 Mean Ranks – Benefits of Personalisation

Ranks	
	Mean Rank
O1_Q2_SAVE-TIME	2.07
O1_Q2_BETTER_CONTENT	2.29
O1_Q2_RELEVENT_ADS	2.85
O1_Q2_USER_EXPERIANCE	2.78

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

Students ranked "Saves Time" as the most important benefit (Mean Rank = 2.07), followed by "Better Content Recommendations." "Relevant Advertisements" received the lowest priority.

Interpretation:

Although correlation analysis did not show statistically significant relationships, ranking analysis indicates that students clearly recognize data collection practices and strongly value convenience. This behavioral insight supports the presence of personalisation-driven preferences.

b. Impact of Digital Literacy on Informed Consent

To assess the impact of digital literacy on informed consent decisions.

Multiple Regression Analysis:

A regression analysis was conducted to examine whether digital literacy significantly predicts informed consent understanding.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Table 6 ANOVA Table – Regression Model (Objective 2)

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.667	1	4.667	7.393	.008[b]
	Residual	46.080	73	.631		
	Total	50.747	74			
a. Dependent Variable: DL1						
b. Predictors: (Constant), CU1						

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

The ANOVA result shows:

F = 7.393

p = 0.008

Since the p-value is less than 0.05, the regression model is statistically significant.

Hypothesis Testing:

H02: There is **no significant impact** of digital literacy on informed consent.

H12: There is a significant impact of digital literacy on informed consent.

Because **p = 0.008 is less than 0.05,** the null hypothesis is rejected and the **alternative hypothesis is accepted**. **Interpretation**

The findings indicate that digital literacy significantly influences informed consent decisions. Students with higher digital knowledge are more likely to understand privacy policies and make informed decisions before accepting terms and conditions.

Ranking Analysis:

Companies Whose Privacy Policies Are Best Understood

Table 7 Mean Ranks – Privacy Policy Understanding

Ranks	
	Mean Rank
O2_Q1_GOOGLE	1.80
O2_Q1_INSTAGRAM	2.51
O2_Q1_WHATSAPP	2.28
O2_Q1_AMAZON	3.41

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

Google received the best rank (1.80), indicating that students feel they understand its policies better than others. Amazon received the lowest rank.

The Friedman test was statistically significant ($p < 0.001$).

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Factors Influencing "Accept" Decisions

Table 8 Mean Ranks – Factors Influencing Consent

Ranks	
	Mean Rank
O2_Q2_LENGHT	1.91
O2_Q2_LANGUAGE	2.33
O2_Q2_TIME_PRESSURE	2.75
O2_Q2_TRUST	3.01

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

The **length of the policy** was ranked as the most influential factor, followed by technical language.

The result was statistically significant ($p < 0.001$).

Interpretation:

Ranking results reinforce the regression findings by showing that structural elements such as length and complexity of policies influence consent behaviour.

c. Gap Between Privacy Concern and Actual Online Behaviour

To examine the gap between students' privacy concerns and their actual online behaviour.

Descriptive Statistics:

Table 9 Descriptive Statistics – Privacy Concern and Actual Behaviour

One-Sample Test							
	Test Value = 0						
	t	xdf	Significance		Mean Difference	95% Confidence Interval of the Difference	
			One-Sided p	Two-Sided p		Lower	Upper
PC1	46.679	74	<.001	<.001	4.160	3.98	4.34
AB2	23.755	74	<.001	<.001	3.147	2.88	3.41

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

The **mean score for Privacy Concern was 4.16**, indicating high concern. The **mean score for Actual Behaviour was 3.15,** reflecting moderate privacy- protective actions.

The difference between means suggests a behavioural gap.

The results also show statistically **significant values ($p < 0.001$)**, confirming the **existence of a gap between expressed concern and actual behaviour**. **Hypothesis Testing**

H03: There is **no significant gap** between privacy concern and actual online behaviour.

H13: There is **a significant gap** between privacy concern and actual online behaviour.

Since $p < 0.05$, the null hypothesis (H03) is rejected and alternative hypothesis (H13) is accepted

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Interpretation:

The findings confirm that students express strong privacy concerns but do not consistently translate those concerns into protective online actions. This supports the existence of a privacy behaviour gap.

Ranking Analysis:

Most Frequent Risky Behaviours

Table 10 : Mean Ranks – Risky Online Behaviours

Ranks	
	Mean Rank
O3_Q1_SAME_PASSWORD	1.57
O3_Q1_UNKOWN_LINKS	2.47
O3_Q1_ACCEPT_WITHOUT_READ	2.71
O3_Q1_PUBLICSHARE	3.25

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

Using the same password across accounts was ranked as the most frequent behaviour.

Reasons for Not Managing Privacy Settings

Table 11 Mean Ranks – Reasons for Not Managing Privacy

Ranks	
	Mean Rank
O3_Q2_LACK_OF_TIME	1.78
O3_Q2_LACK_OF_KNOLEDGE	2.42
O3_Q2_FEEL_COMPLICATED	2.68
O3_Q2_TRUST_PLATFORM	3.12

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

Lack of time was ranked as the primary reason.

Table 12 Friedman Test Statistics

Test Statistics	
N	75
Kendall's W[a]	.213
Chi-Square	47.860
df	3
Asymp. Sig.	<.001

a. Kendall's Coefficient of Concordance

(Source: Primary data collected through questionnaire and analysed by SPSS tools)

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Both Friedman tests were statistically significant ($p < 0.001$).

1. ***Secondary data analysis (Qualitative Case Review)***

In this section, qualitative insights are presented from selected real-world privacy and data breach cases. The primary data findings are supported by illustrating how large-scale privacy incidents are reflected in similar behavioural patterns observed among college students.

Table 13 Summary of secondary data

Case	Core Privacy Issue	Key Qualitative Insight (Student Perspective)
K.S. Puttaswamy v. Union of India (Aadhaar Data Breach)	Unauthorized access to personal and biometric data	Students view large-scale data collection as unavoidable and accept privacy loss in exchange for convenience and access
Pegasus Spyware Scandal (2021)	State surveillance and lack of consent	Students expressed fear of surveillance but felt powerless to control or resist digital monitoring
Star Health Insurance Data Leak (2024)	Exposure of sensitive health and financial data	High concern over health data misuse, yet continued usage of digital health services due to necessity
Policybazaar Data Breach (2022)	Fintech system vulnerability and data negligence	Students routinely accepted privacy policies without reading despite awareness of risks
Cambridge Analytica – India Connection	Manipulative political micro- targeting	Students recognized targeted content but underestimated its influence on attitudes and choices

(Source: various news articles)

The qualitative case analysis reveals consistent themes across major data breach and surveillance incidents. In cases such as K.S. Puttaswamy v. Union of India and the Pegasus Spyware Scandal, students acknowledged privacy risks yet demonstrated a sense of inevitability and limited behavioural change. Similarly, data breaches like Star Health Insurance and Policy bazaar indicate awareness of risks but continued digital engagement due to convenience and necessity. These insights reinforce the personalisation–privacy paradox and confirm the privacy concern–behaviour gap identified in the primary data analysis.

2. ***Summary of Findings***

The findings of the study combine insights from both quantitative and qualitative analysis to present a clear understanding of students' privacy attitudes and digital behaviour.

The primary data shows that no statistically significant relationship exists among Privacy Concern, Perceived Benefits of Personalisation, and Privacy Protection Behaviour, indicating that awareness and perceived

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

advantages of personalisation do not directly shape protective actions. However, Digital Literacy significantly influences Informed Consent Understanding, suggesting that digitally aware students are better able to comprehend consent mechanisms. The analysis also confirms a significant gap between Privacy Concern and Actual Online Behaviour, demonstrating that expressed concerns do not consistently translate into cautious online practices. Ranking results further highlight behavioural patterns such as preference for convenience, influence of policy length, password reuse, and lack of time in managing privacy settings.

The secondary case review, including instances such as K.S. Putta swamy v. Union of India and the Pegasus spyware scandal, supports these findings by showing that students recognize privacy risks but continue digital engagement due to convenience, necessity, or limited alternatives.

Overall, the integrated findings confirm the presence of a privacy concern behaviour gap and reflect the continuing personalisation privacy tension among college students despite growing digital awareness.

3. *Proposed Strategic Framework – PSMM*

Privacy Segmented Marketing Model

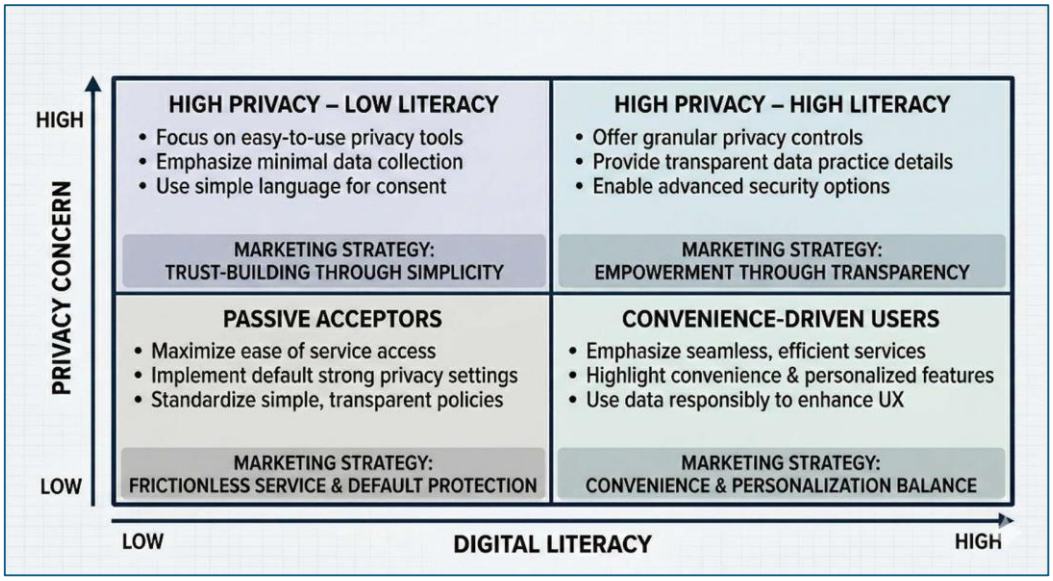


Figure 3 PSMM model

The Privacy Segmented Marketing Model (PSMM) proposes that startups segment customers based on a Privacy Sensitivity Index rather than only demographics. Based on digital literacy and privacy concern levels, users are grouped into four segments: High Privacy - Low Sharing, High Privacy - High Literacy, Convenience Driven Users, and Passive Acceptors. Each segment receives a tailored personalisation strategy. High Literacy users are offered detailed customization controls, Convenience-Driven users receive frictionless personalisation, and High Privacy users are given limited tracking with opt-in options. This model enables ethical targeting, strengthens trust based branding, reduces churn, and helps startups align data - driven marketing with user comfort levels.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

Conclusion:

The study examined the personalisation–privacy paradox among college students, focusing on how their privacy awareness, perceived online advantages and digital skills influence what they do online. The findings show no significant relationship between privacy concern and privacy protection behaviour, indicating that awareness alone does not influence protective actions. The level of digital literacy greatly shapes how well students understand informed consent, suggesting that those with higher digital proficiency make more informed online choices. The study also highlights a noticeable gap between what students say about their privacy and how they actually behave online. Although students understand potential online risks, they persist in convenience- oriented habits. The study underscores the persistent gap between privacy awareness and actual behaviour and advocates for enhanced digital skills and more transparent consent practices to promote accountable online participation.

References:

1. *Acquisti, B. &. (2015). Retrieved from https://www.science.org/doi/10.1126/science.aaa1465*
2. *al., T. e. (2017). Retrieved from https://www.researchgate.net/publication/367617505_The_privacy_calculus_contextualized-The_influence_of_affordances*
3. *Baban K. More, D. S. (2020). Retrieved from https://www.researchgate.net/profile/Baban-More-4/publication/349589226_Development_of_information_and_digital_literacy_skills_among_management_institute_Library_users_A_study_affiliated_to_the_University_of_Mumbai/links/6037584ea6fdcc37a84dfcdd/Developme*
4. *jong, B. a. (2017). Retrieved from https://www.sciencedirect.com/science/article/pii/S0736585317302022*
5. *Livingstone, v. c. (2018). Retrieved from https://www.researchgate.net/publication/241424456_Converging_traditions_of_research_on_media_and_information_literacies_Disciplinary_critical_and_ methodological_issues*
6. *Tara van Dijk, A. B. (2016). Retrieved from https://journals.sagepub.com/doi/abs/10.1177/2233865916628701*
7. *Vashistha, A. (2018). Retrieved from https://dl.acm.org/doi/abs/10.1145/3209811.3209818*

Cite This Article:

Pathan A., Shaikh S., Yadav S. & Dr. Shukrey M. (2026). *Convenience vs. Consent: Exploring the Personalisation-Privacy Paradox in the Daily Digital habits of College Students.* **In Educreator Research Journal: Vol. XIII (Issue I),** pp. 188–200. **Doi: https://doi.org/10.5281/zenodo.19883229**