

International Research Journal of Business and Social Science

Volume: 12 Issue: 4
October-December, 2026
ISSN:2411-3646



Research Article

Data Privacy Concerns and Consumer Engagement with AI-Enabled Global Digital Platforms in Bangladesh: The Mediating Role of Perceived Trust

Mst. Tahsina Jannat^{1*}; Atifa Akter Juthy¹; Sraboni Akter¹; Kazi Abdul Mannan²

^{1*}Department of Computer Science & Technology

²Department of Business Administration

Shanto-Mariam University of Creative Technology, Uttara, Dhaka, Bangladesh

ABSTRACT

This study examines how data privacy concerns shape consumer engagement with AI-enabled global digital platforms in Bangladesh and tests perceived trust as an intervening mechanism. The study responds to the rapid normalization of data-intensive platform services in an emerging digital economy, where privacy concern, trust and continued participation coexist rather than operate as simple opposites. A quantitative cross-sectional survey design was used. Of 400 database rows, 385 complete cases passed the embedded attention check and were retained. Privacy concern, perceived trust and consumer engagement were measured with three five-point Likert items each. Composite-score regression and non-parametric bootstrap mediation were used as a transparent robustness-oriented analysis because the three-item scales displayed only modest internal consistency. Privacy concern was positively associated with trust ($b=0.164$, $p=0.006$); trust, in turn, was positively associated with engagement while controlling for privacy concern ($b=0.231$, $p<.001$). The total privacy-concern-engagement association was small but significant ($b=0.117$, $p=0.026$), whereas the direct effect became non-significant after trust entered the model ($b=0.079$, $p=0.123$). The bootstrapped indirect effect was 0.038, 95% CI [0.010, 0.072], indicating an indirect pathway through trust. These results reveal a contextually important privacy-trust-engagement configuration, but the modest reliability of the short scales requires cautious interpretation. The article therefore contributes both substantive evidence and a measurement lesson for platform research in Bangladesh: privacy salience may coexist with engagement when users retain confidence in established platforms, yet stronger validated measures are needed before definitive causal or theory-confirming claims are made.

ARTICLE HISTORY

Received 10 September 2026

Revised 28 October 2026

Accepted 02 October 2026

KEYWORDS

privacy calculus; digital trust; consumer engagement; global digital platforms; artificial intelligence; Bangladesh; mediation

CONTACT Mst. Tahsina Jannat, Email: tahsinajannat9484@gmail.com

1. Introduction

This section establishes the scholarly and contextual basis of the study. It first situates data privacy, trust, and consumer engagement within the expanding ecosystem of AI-enabled global digital platforms, and then narrows the discussion to Bangladesh as an emerging digital market. Building on this context, the section identifies the practical and theoretical problem, specifies the unresolved empirical gap, states the research objectives and question, and clarifies the study's intended contribution and overall structure.

Global digital platforms increasingly mediate communication, commerce, learning, entertainment, payments and access to information. Their value creation depends heavily on data collection, algorithmic personalization and automated decision processes. These capabilities can improve convenience and relevance, but they also make privacy a central condition of platform relationships. Privacy is no longer a peripheral compliance issue: it is part of the consumer's assessment of whether a platform is sufficiently trustworthy to deserve attention, data, time and repeated participation [1]-[6]. AI-enabled services intensify this tension because personalization and prediction can make data practices less visible even while making services more useful.

Bangladesh provides a consequential setting for this problem. The Bangladesh Telecommunication Regulatory Commission reported 128.27 million internet subscriptions in February 2026, while total internet penetration was reported at 74.52% in April 2026 [7], [8]. These indicators describe subscriptions and penetration rather than unique individual users,

but they demonstrate the scale at which digital platforms are embedded in the national economy. The expansion of platform use creates opportunities for digital inclusion and productivity while simultaneously increasing exposure to opaque data collection, secondary use, profiling and security risks. Recent Bangladesh research also shows that trust, privacy and perceived security are intertwined in digital financial and e-government contexts [9], [10].

The practical problem is not simply whether consumers are concerned about privacy. Consumers can remain highly active on platforms while expressing substantial concern about data collection and secondary use. This apparent inconsistency is often described as the privacy paradox, although privacy-calculus research suggests that behavior may reflect a conditional trade-off among benefits, risks, habits, context and trust rather than irrationality [1], [2], [11]. For platform managers, the unresolved issue is therefore mechanistic: through what pathway do privacy concerns translate into lower, unchanged or even higher engagement? If trust functions as a relational assurance mechanism, consumers may remain engaged despite privacy salience; if trust deteriorates, the same privacy concern may suppress participation.

Three gaps motivate this study. First, much privacy research concentrates on disclosure intention, adoption or continuance rather than consumer engagement as a broader behavioral orientation involving interaction, time and deeper participation [3], [12]-[15]. Second, studies often model privacy concern and trust as parallel predictors rather than explicitly testing trust as the mechanism linking privacy concern to engagement. Third, Bangladesh-specific empirical evidence remains concentrated in

particular domains such as digital finance, e-commerce and public digital services [9], [10], [16], leaving cross-platform consumer ecosystems comparatively underexamined. The present study addresses these gaps using a parsimonious mediation model grounded in Privacy Calculus Theory and Trust Theory.

The general objective is to examine the relationship between privacy concern and consumer engagement with global digital platforms in Bangladesh, with perceived trust tested as a mediator. Specifically, the study assesses (i) the privacy concern-trust relationship, (ii) the trust-engagement relationship, (iii) the direct and total association between privacy concern and engagement, and (iv) the indirect effect through trust. The corresponding research question is: To what extent does perceived trust explain the relationship between privacy concern and consumer engagement among adult users of global digital platforms in Bangladesh?

The study's novelty lies in combining a privacy-calculus lens with a trust-mediated engagement mechanism in an emerging-economy, cross-platform setting. It moves beyond a binary assumption that privacy concern necessarily causes disengagement. Empirically, it uses a 385-case primary dataset and reports the indirect pathway alongside scale diagnostics rather than suppressing measurement weaknesses. Contextually, it adds evidence from Bangladesh at a time of rapid platform diffusion. Methodologically, the analysis demonstrates why reliability and construct validity must be considered before interpreting statistically significant structural relationships as strong theoretical confirmation.

The remainder of the article reviews privacy calculus, trust and engagement research,

develops the hypotheses and conceptual model, explains the research design and analytical strategy, reports empirical results, interprets the findings, develops theoretical and practical implications, and concludes with limitations and future research priorities.

2. Literature Review and Theoretical Foundation

To develop a theoretically coherent explanation of the focal relationships, this section synthesizes literature on information privacy, platform trust, and consumer engagement rather than treating these constructs as isolated concepts. The review is anchored in Privacy Calculus Theory and Trust Theory, which together provide the logic for explaining why privacy-aware users may either restrict or sustain engagement depending on the confidence they place in a platform. The section proceeds from conceptual foundations to theory integration, construct-specific evidence, hypothesis development, and the resulting conceptual framework.

2.1 Privacy in AI-Enabled Digital Platform Ecosystems

Digital platforms create value by coordinating users, content, services and data. AI expands this architecture through recommender systems, automated classification, prediction and personalization. Such systems can improve relevance and efficiency while increasing informational asymmetry: firms may know substantially more about the consumer than the consumer knows about the platform's data practices. Information privacy research consequently treats privacy concern as a multidimensional response to collection, unauthorized secondary use, improper access and errors in personal information [17], [18].

Contemporary privacy calculus research further emphasizes that disclosure and participation are context-dependent and not reducible to a fully rational cost-benefit calculation [1], [2].

2.2 Privacy Calculus Theory

Privacy Calculus Theory proposes that individuals evaluate expected benefits of disclosure or participation against perceived privacy risks and costs [11], [19]. The theory has been widely applied to e-commerce, social media, mobile services and personalized advertising. Recent work argues that the calculus can be habitual, affective and context sensitive rather than strictly deliberative [1]. This refinement is important for mature digital platforms: users may perceive privacy risk yet continue to participate because switching costs, social value, convenience, personalization and accumulated trust alter the net evaluation. The present study therefore does not assume that privacy concern must have a uniformly negative observed association with engagement.

2.3 Trust Theory

Trust reduces perceived vulnerability in relationships characterized by uncertainty and dependence [20]-[23]. In online environments, trust reflects confidence that a provider is reliable, competent and sufficiently responsible in handling users and their information. Trust is especially relevant where consumers cannot directly inspect algorithms, security controls or downstream data use. Prior studies show that provider trust can increase disclosure, adoption, continuance and engagement and can alter the behavioral consequences of privacy concern [3], [13], [14]. In Bangladesh, recent research similarly identifies trust as a central component of digital-service adoption [9], [10], [16].

2.4 Consumer Engagement

Consumer engagement captures active interaction and investment in a focal platform or brand beyond a single transaction. Digital engagement can involve frequency of interaction, time spent, participation, contribution and willingness to deepen use [24]-[27]. The survey instrument operationalizes engagement as active interaction with trusted platforms, spending more time where experiences are valuable and trustworthy, and willingness to participate more deeply when privacy and trust expectations are met. This formulation makes engagement relational and conditional, which is theoretically compatible with a trust-mediated privacy mechanism.

2.5 Hypotheses Development

Privacy concern signals that users are attentive to how personal information is collected and used. Classical privacy-risk reasoning predicts that greater concern should erode confidence where platforms are perceived as intrusive. However, mature platform relationships can generate a different empirical pattern: privacy-aware users may selectively remain with reputable platforms, use privacy controls, or concentrate activity where they perceive stronger institutional assurance. Research on the privacy paradox and contextual privacy calculus supports the possibility that concern and use can coexist [1], [3], [28]. The study therefore tests the empirical association without treating a negative sign as inevitable. H1: Privacy concern is significantly associated with perceived trust in global digital platforms.

Trust provides a basis for accepting vulnerability and continuing interaction under uncertainty. When consumers believe a platform is reliable and handles user interests responsibly, they should be more willing to invest time,

interact actively and deepen participation. Evidence across social media, e-commerce and digital services consistently links trust with behavioral intention and engagement [3], [10], [13], [20]. H2: Perceived trust is positively associated with consumer engagement.

Privacy concern can also influence engagement directly. Higher concern may encourage protective withdrawal, lower contribution and reduced digital consumption; recent panel evidence and earlier social-network research support such a negative pathway [4], [29]. Conversely, privacy-aware consumers may remain engaged when they perceive adequate benefits and controls. H3: Privacy concern is significantly associated with consumer engagement.

Integrating Privacy Calculus Theory with Trust Theory suggests that privacy concern may affect engagement partly through the consumer's confidence in the platform. Trust can translate assessments of vulnerability into willingness to participate. Prior work has identified trust as a mediator in privacy and disclosure processes [13], [30]. H4: Perceived trust mediates the relationship between privacy concern and consumer engagement.

2.6 Conceptual Framework

The conceptual framework in Figure 1 translates the theoretical integration into a testable mediation model. Privacy concern (PC) is positioned as the exogenous focal construct

because Privacy Calculus Theory begins with the user's assessment of informational vulnerability, collection and secondary use. Perceived trust (TR) occupies the mediating position because Trust Theory explains how users convert uncertainty about a platform into a relational judgment about reliability and responsible conduct. Consumer engagement (CE) is the endogenous outcome, reflecting the extent to which users interact, spend time and deepen participation on platforms. The model therefore separates a privacy appraisal from the relational assurance mechanism through which that appraisal may become behaviorally consequential.

The arrows in Figure 1 represent four analytically distinct propositions. H1 links privacy concern to perceived trust and tests whether privacy salience is associated with the user's confidence in established platforms. H2 links trust to engagement and represents the core trust-theoretic expectation that confidence reduces perceived vulnerability and supports continued participation. H3 retains a direct PC→CE path so that privacy concern can influence engagement independently of trust. H4 is the indirect PC→TR→CE pathway: it tests whether trust carries part or all of the statistical association between privacy concern and engagement. Retaining both the direct and indirect paths is important because it allows the study to distinguish a simple privacy-effect model from a mediated relational mechanism.

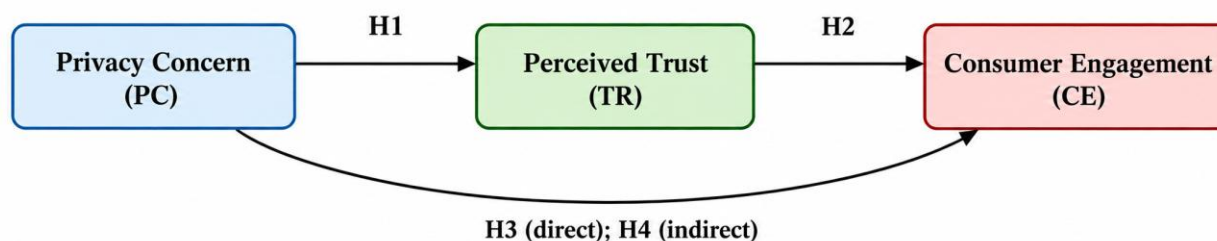


Figure 1. Proposed privacy concern-trust-consumer engagement framework

Conceptually, the framework should not be read as assuming that greater privacy concern must automatically reduce engagement. Privacy-calculus reasoning permits competing behavioral responses: concern may generate withdrawal, but privacy-aware users may also remain active when they perceive adequate benefits, controls and trustworthy institutional conduct. Accordingly, the signs and magnitudes of H1 and H3 are treated as empirical questions, whereas H2 is theoretically expected to be positive. Evidence for H4 requires the estimated indirect effect to differ from zero. This interpretation is especially important in the Bangladesh context, where global platforms can be highly embedded in everyday digital activity and users may simultaneously report privacy concern and continued participation.

3. Methodology

This section explains how the proposed relationships were examined empirically and how the collected survey data were prepared for analysis. The methodological choices are aligned with the study's cross-sectional quantitative design and focal constructs. Particular attention is given to respondent eligibility, sample retention, measurement selection, data screening, analytical procedures,

and ethical considerations so that the empirical claims can be evaluated in light of both the strengths and limitations of the research design.

3.1 Research Design and Context

The study adopted a quantitative, cross-sectional and explanatory survey design. The unit of analysis was the individual adult user of global digital technology platforms in Bangladesh. The design was selected because the research problem concerns associations among latent-style perceptual constructs measured at one point in time. The study should therefore be interpreted as associational rather than causal: temporal ordering cannot be established from a cross-sectional dataset.

3.2 Population, Eligibility and Sampling

The target population comprised adults in Bangladesh who regularly use major global digital platforms and are familiar with privacy or data-sharing features. The study used purposive/criterion-based screening, with a target of 400 responses and retention of at least 385 valid cases, consistent with the large-population Cochran benchmark at 95% confidence, 5% margin of error and $p=.50$. The collected dataset contained 400 respondent IDs; 385 rows contained complete scale responses and the required attention-check value of 4

(“Agree”), while 15 trailing rows were unfilled. Accordingly, the empirical sample is $n=385$. Because recruitment was non-probability based, Cochran’s figure should be understood as a size benchmark rather than evidence of probability-sampling representativeness.

3.3 Instrument and Measurement

The survey instrument contained multiple constructs related to digital-platform use and consumer perceptions. Consistent with the objectives of the present study, the analysis focuses on Privacy Concern (PC1-PC3), Digital Trust/Perceived Trust (TR1-TR3 in the dataset; DT1-DT3 in the questionnaire wording) and Consumer Engagement (CE1-CE3). All items use a five-point Likert response format. PC1 addresses concern about collection of personal information, PC2 concern about secondary data use, and PC3 whether privacy concerns affect active engagement. Trust items capture platform reliability, responsible data handling and confidence in relying on established platforms. Engagement items capture active interaction, time spent and deeper participation under privacy/trust expectations.

A measurement caveat is essential. PC3 embeds a behavioral consequence (“affect how actively I engage”) within the privacy-concern scale, while CE items also contain explicit trust/privacy conditions. This creates conceptual proximity between predictor, mediator and outcome. The issue is reported transparently because it can inflate or alter observed relationships and should be corrected in a future instrument-validation study.

3.4 Data Screening and Analysis

Rows were retained when the attention check equaled 4 and all focal construct items were present, yielding 385 usable cases. Descriptive statistics and bivariate correlations were

computed. Internal consistency was assessed with Cronbach’s alpha. Because the alpha values were modest and the short scales did not meet conventional thresholds for strong internal consistency, the primary structural analysis uses mean composites and ordinary least-squares regression rather than treating the measures as well-validated latent constructs. Mediation was tested using the product-of-coefficients logic with 2,000 non-parametric bootstrap resamples and a 95% percentile confidence interval. The indirect effect is interpreted as statistically detectable when its confidence interval excludes zero. This strategy prioritizes transparent inference over overclaiming model precision.

3.5 Ethical Considerations

The questionnaire states that participation is voluntary, respondents are adults, responses are for academic research, and consent is required. The collected dataset contains respondent IDs but no direct names, email addresses or telephone numbers. The study was conducted as a non-clinical, minimal-risk academic field exercise involving adult participants and did not involve any medical intervention, clinical procedure, collection of biological materials, or personally identifying information. At the time of data collection, no dedicated institutional ethics review mechanism or formal approval number was available for this course-based research within the researchers’ institutional setting. Accordingly, the study was conducted in accordance with internationally recognized principles for research involving human participants, including voluntary participation, prior informed consent, anonymity, confidentiality, the right to decline or discontinue participation, and the use of collected data solely for academic research purposes. No directly identifying personal information was collected or reported, and the

dataset was handled in a manner intended to protect participants' privacy and confidentiality.

4. Results

This section reports the empirical evidence in a sequential manner, moving from sample characteristics and construct-level diagnostics to bivariate relationships and hypothesis testing. Consistent with good quantitative reporting practice, interpretation is kept limited here; the purpose is to establish what the data show before explaining why the observed patterns may have occurred. Because the focal scales display modest internal consistency, the results also distinguish carefully between statistically

detectable composite-score relationships and stronger claims that would require a well-validated latent measurement model.

4.1 Respondent Profile

Before examining relationships among the focal constructs, the composition of the analytical sample is described to establish the demographic and digital-use context in which the model is estimated. Table 1 summarizes age, gender, current status, education, platform-use frequency, length of experience and experience with AI-enabled features for the 385 retained respondents.

Table 1. Demographic and Digital-Use Profile of Respondents

Characteristic	Category	n	%
Age-Group	21-25	171	44.4%
Age-Group	26-30	82	21.3%
Age-Group	31-40	59	15.3%
Age-Group	18-20	58	15.1%
Age-Group	41 or above	15	3.9%
Gender	Male	215	55.8%
Gender	Female	160	41.6%
Gender	Prefer not to say	6	1.6%
Gender	Prefer to self-describe	4	1.0%
Current-Status	Student	178	46.2%
Current-Status	Employed	130	33.8%
Current-Status	Self-employed/Freelancer	59	15.3%
Current-Status	Other	18	4.7%
Education-Level	Undergraduate	169	43.9%
Education-Level	Graduate	106	27.5%
Education-Level	Postgraduate	88	22.9%
Education-Level	Other	22	5.7%
Use-Frequency	Daily	240	62.3%
Use-Frequency	Several times/week	102	26.5%
Use-Frequency	Weekly	36	9.4%
Use-Frequency	Less often	7	1.8%
Experience-Length	>5 years	160	41.6%
Experience-Length	3-5 years	123	31.9%
Experience-Length	1-2 years	54	14.0%
Experience-Length	6-12 months	31	8.1%
Experience-Length	<6 months	17	4.4%

Characteristic	Category	n	%
AI-Feature-Experience	Regular user	150	39.0%
AI-Feature-Experience	Occasional user	147	38.2%
AI-Feature-Experience	Aware but not used	66	17.1%
AI-Feature-Experience	Not sure/not aware	22	5.7%

Table 1 indicates that the dataset primarily represents young, highly connected and experienced digital-platform users. This profile is substantively relevant because frequent and long-term exposure can simultaneously increase awareness of privacy risks and familiarity with platform safeguards. Consequently, the subsequent privacy-trust-engagement estimates should be interpreted as relationships observed among comparatively digitally engaged users rather than as nationally representative population parameters.

The sample was concentrated among younger and digitally active users. Respondents aged 21-25 formed the largest age group (44.4%), followed by ages 26-30 (21.3%). Men represented 55.8% and women 41.6%. Students comprised 46.2% and employed respondents 33.8%. Daily platform users accounted for 62.3% of the sample. Experience was substantial: 41.6% reported more than five years of relevant technology/service experience and 31.9% reported three to five years. Regarding AI-feature experience, 39.0% identified as regular users and 38.2% as occasional users.

4.2 Construct Descriptives and Reliability

Table 2 reports the central tendency, dispersion and internal-consistency estimates for the focal constructs. These statistics provide the first assessment of how strongly respondents endorsed privacy concern, trust and engagement and whether the three-item measures behaved

coherently enough to support subsequent composite-score analysis.

Table 2. Descriptive Statistics and Internal Consistency of Focal and Robustness Constructs

Construct	Mean	SD	Cronbach α
Privacy Concern	3.998	0.475	0.473
Perceived Trust	3.678	0.552	0.537
Consumer Engagement	3.980	0.488	0.448
Privacy Control	3.460	0.496	0.414

As shown in Table 2, privacy concern and consumer engagement both cluster near the 'agree' region of the scale, while trust is somewhat lower but still above the midpoint. The alpha coefficients, however, are below conventional confirmatory thresholds. This result materially shapes the analytical strategy: the manuscript does not portray these measures as strongly validated latent variables, and the regression/mediation results are interpreted cautiously as composite-score associations.

Privacy concern and consumer engagement were both high on the five-point scale ($M=3.998$ and 3.980 respectively), while perceived trust was moderately high ($M=3.678$). Internal consistency, however, was weak-to-marginal: $\alpha=.473$ for privacy concern, $\alpha=.537$ for trust and $\alpha=.448$ for engagement. These values are below conventional confirmatory-research expectations. The structural coefficients should

therefore be interpreted as relationships among observed composite indices rather than as precise estimates among well-validated latent variables.

4.3 Correlations

Bivariate correlations were examined before multivariable modeling to assess the direction and approximate magnitude of the zero-order relationships and to identify whether the constructs exhibited extreme overlap. Table 3 presents the Pearson correlations among privacy concern (PC), perceived trust (TR), consumer engagement (CE) and perceived privacy control (PPC).

Table 3. Pearson Correlation Matrix for Focal and Robustness Constructs

Variables	PC	TR	CE	PPC
PC	1.000	0.141	0.114	0.502
TR	0.141	1.000	0.273	0.096
CE	0.114	0.273	1.000	0.164
PPC	0.502	0.096	0.164	1.000

Table 3 shows that PC has weak positive zero-order relationships with TR and CE, whereas the TR-CE association is noticeably stronger. The PC-PPC correlation is the largest in the matrix but remains well below a level that would indicate near-duplication. These patterns

provide preliminary support for testing trust as an intervening variable while also suggesting that privacy concern alone explains only a small share of engagement variation.

Privacy concern correlated positively but weakly with trust ($r=.141$) and engagement ($r=.114$). Trust showed a stronger positive correlation with engagement ($r=.273$). Privacy concern correlated substantially with perceived privacy control ($r=.502$), suggesting that respondents who were more privacy attentive also tended to report greater concern/control salience. This pattern is compatible with a privacy-management interpretation rather than a simple withdrawal model.

4.4 Hypothesis Tests and Mediation

The hypothesized relationships were then tested sequentially. The first regression estimates the PC→TR path; the second estimates engagement from PC and TR simultaneously; a separate total-effect model estimates PC→CE before the mediator is introduced. The indirect effect was evaluated with 2,000 bootstrap resamples. Table 4 integrates the coefficients, significance tests, explanatory power and mediation interval so that the direct, total and indirect relationships can be evaluated together.

Table 4. Structural Regression Paths and Bootstrap Mediation Results

Test	Path	b / indirect	t	p	R ² / CI	Result
H1	PC → TR	0.164	2.791	0.006	0.020	Significant
H2	TR → CE PC	0.231	5.282	<.001	0.080	Supported
H3	PC → CE (total)	0.117	2.236	0.026	0.013	Significant
Direct	PC → CE TR	0.079	1.544	0.123	0.080	Not significant
H4	PC → TR → CE	0.038	-	-	95% CI [0.010, 0.072]	Indirect effect detected

The pattern in Table 4 is theoretically informative. PC significantly predicts TR, and TR significantly predicts CE when PC is held constant. Although the total PC→CE association is statistically significant, the direct PC→CE coefficient is reduced and becomes non-significant after TR enters the model. At the same time, the bootstrap confidence interval for the indirect effect excludes zero. Taken together, the estimates are consistent with an indirect-only mediation pattern in the fitted composite-score model: the observed association between privacy concern and engagement is statistically transmitted primarily through perceived trust. Because the measures have modest reliability and the data are cross-sectional, this pattern should be interpreted as evidence of an indirect statistical mechanism rather than proof of causal mediation.

H1 was statistically significant: privacy concern was positively associated with perceived trust ($b=0.164$, $SE=0.059$, $t=2.791$, $p=0.006$), although explanatory power was low ($R^2=0.020$). H2 was supported: perceived trust positively predicted engagement after controlling for privacy concern ($b=0.231$, $SE=0.044$, $t=5.282$, $p<.001$). The two-predictor engagement model explained 8.0% of observed variance.

For H3, the total association between privacy concern and engagement was small and positive ($b=0.117$, $p=0.026$, $R^2=0.013$). Once trust was entered, the direct privacy-concern coefficient declined to $b=0.079$ and was no longer statistically significant ($p=0.123$). The bootstrapped indirect effect through trust was 0.038, with a 95% CI of [0.010, 0.072]. Because the interval excludes zero, H4 receives statistical support at the composite-score level. The pattern is consistent with indirect-only mediation in the fitted model, but the low reliability and item

overlap prevent a strong causal or latent-construct claim.

4.5 Exploratory Privacy-Control Robustness Check

Because the questionnaire also measures perceived privacy control, an exploratory first-stage moderation check was conducted to determine whether privacy control altered the privacy concern-trust association. The interaction was small and non-significant ($b=.014$, $p=.564$). This analysis is not part of the preregistered focal model and is therefore treated as exploratory. It suggests that the observed mediation pattern cannot be straightforwardly attributed to a simple concern-by-control interaction in this dataset.

4.6 Summary of Findings

The data produce four central findings. First, privacy concern was high but did not correspond to lower engagement. Second, privacy concern showed a small positive association with perceived trust. Third, trust was the strongest focal predictor of engagement. Fourth, the privacy concern-engagement total association became non-significant after trust was controlled, while the bootstrapped indirect effect remained above zero. These results point to a privacy-salience-trust-engagement configuration rather than a simple privacy-concern-withdrawal relationship.

5. Discussion

The preceding results reveal a pattern that is more nuanced than a simple assumption that stronger privacy concern necessarily reduces digital-platform engagement. This section interprets those findings through Privacy Calculus Theory and Trust Theory, relates them to prior empirical research, and considers the

specific conditions of Bangladesh's rapidly expanding digital environment. Particular emphasis is placed on the positive privacy concern-trust relationship, the stronger role of trust in explaining engagement, the observed indirect pathway, and the measurement features that require caution when drawing substantive conclusions.

5.1 Privacy Concern Does Not Necessarily Mean Withdrawal

The positive total association between privacy concern and engagement differs from the common expectation that concern suppresses digital participation. Studies have found negative associations between privacy concerns and social-network engagement or digital consumption [4], [29]. Yet the privacy paradox literature warns against assuming a one-directional relationship between concern and behavior [1], [28]. In a highly embedded platform environment, privacy-aware users may continue using services because benefits, habits, network effects and switching costs remain substantial. The present result is therefore better interpreted as coexistence of privacy salience and platform participation than as evidence that privacy concern causes engagement.

5.2 Trust as the Central Relational Mechanism

Trust was positively and more strongly related to engagement than privacy concern. This accords with Trust Theory: where users face uncertainty about data practices, algorithms and institutional behavior, confidence in the provider reduces perceived vulnerability and enables deeper participation [20]-[23]. The result is also consistent with research showing that social-media trust can sustain engagement despite privacy concern [3]. In Bangladesh, where digital platforms are expanding rapidly,

trust may be particularly consequential because users interact with complex multinational data ecosystems whose governance processes are difficult to observe directly.

5.3 Interpreting the Positive Privacy Concern-Trust Path

The positive PC→TR coefficient requires caution. It could indicate selective trust: privacy-conscious consumers may concentrate their activity on established platforms that they believe are more reliable. It could also reflect privacy literacy or greater familiarity-frequent users can simultaneously understand risks and develop calibrated trust. However, a measurement explanation is also plausible. The privacy-concern scale includes PC3, which explicitly states that privacy concerns affect active engagement, while the trust and engagement items contain normative or conditional language about responsible data handling and privacy expectations. Such wording can produce common conceptual variance. The finding should therefore stimulate instrument refinement rather than be treated as a definitive reversal of established privacy-risk theory.

5.4 The Mediation Pattern

The direct privacy concern-engagement coefficient became non-significant after trust entered the model, while the indirect effect was statistically detectable. Mechanistically, this implies that privacy concern is related to engagement primarily through the trust state captured by this instrument. The result aligns with research in which trust mediates privacy-related disclosure processes [13], [30]. It also complements Bangladesh evidence that security and user experience influence trust and that trust subsequently influences adoption [10]. Nevertheless, mediation in cross-sectional data

is statistical rather than temporal; alternative causal orders, such as engagement producing familiarity and trust, remain possible.

5.5 Integrated Interpretation

Collectively, the findings suggest that consumer engagement in global digital ecosystems cannot be explained by privacy concern alone. Privacy-sensitive users appear willing to remain active when they also report trust in platform reliability and responsible data handling. This is consistent with an expanded privacy calculus in which benefits, familiarity and institutional assurance coexist with concern. The model's low R^2 values also indicate that engagement is shaped by many omitted drivers, including usefulness, ease of use, social value, habit, switching costs, platform dependence and perceived benefits. The present parsimonious mediation model should therefore be interpreted as a focused explanatory mechanism rather than a complete theory of consumer engagement.

6. Theoretical and Practical Implications

The empirical findings have implications beyond the individual path coefficients reported above. This section therefore translates the results into three levels of contribution: implications for privacy-calculus and trust-based explanations of digital behavior, implications for managers of global digital platforms, and implications for policy and society in an emerging digital economy. These implications are presented cautiously, recognizing that the study offers a focused mechanism and context-specific evidence rather than a complete model of consumer engagement.

6.1 Theoretical Implications

The first theoretical implication is that privacy concern should not automatically be modeled as behavioral resistance. Privacy calculus is more informative when concern is interpreted within a broader decision context that includes trust, perceived benefits and control. The positive concern-trust association observed here highlights the possibility of privacy-aware trust, where users remain attentive to risk while selectively relying on established providers. Second, the mediation pattern positions trust as a conversion mechanism between privacy assessment and engagement. This extends a simple risk-behavior model toward a relational account: what matters is not only whether consumers perceive privacy risk, but whether the platform relationship provides sufficient assurance to sustain participation. Third, the Bangladesh context demonstrates why theory imported from mature Western markets should be tested rather than assumed. Digital inclusion, platform concentration, cultural expectations and regulatory development can shape the meaning of privacy and trust.

At the same time, the measurement results provide an important theoretical warning. Weak reliability limits the degree to which observed composites can stand in for stable latent constructs. The study therefore contributes by separating statistical significance from measurement adequacy. A theory can only be tested convincingly when constructs are measured distinctly. Future work should use established privacy-concern scales, separate privacy concern from privacy-protective behavior, remove engagement language from predictor items, and ensure that trust items measure trust rather than normative expectations of responsible corporate behavior.

6.2 Managerial Implications

For global platform providers, the findings suggest that privacy communication should be designed to build calibrated trust rather than merely reduce concern. Consumers may remain concerned even when they continue using a service; therefore, low churn should not be interpreted as low privacy risk. Managers should provide intelligible explanations of data collection, secondary use, retention, personalization and AI-enabled processing. Privacy controls should be easy to find, understandable and reversible. Trust can also be strengthened through visible security practices, rapid breach communication, accessible complaint channels and evidence that stated privacy commitments are implemented operationally.

Engagement strategies should avoid exploiting user dependence. If trust is a key pathway to deeper participation, short-term engagement gained through opaque defaults or manipulative consent design may damage the relational mechanism that supports long-term use. Platform teams should monitor trust and privacy perceptions alongside conventional engagement metrics such as session frequency and time spent. In Bangladesh, localized privacy notices and digital-literacy materials in Bangla can reduce comprehension barriers and make privacy choices more meaningful.

6.3 Policy and Societal Implications

Policy should focus on enforceable transparency, meaningful consent, data minimization, security and accessible user rights. Bangladesh's rapidly expanding internet ecosystem increases the social importance of trustworthy data governance. Regulators, educators and civil-society organizations can also strengthen privacy literacy so that users

understand both risks and available controls. Importantly, consumer education should not shift responsibility entirely onto individuals; platform design and institutional accountability remain central because users cannot independently audit complex AI and data infrastructures.

7. Conclusion, Limitations and Future Research

This final substantive section consolidates the study's argument by returning to the research problem, the trust-mediated analytical model, and the principal empirical findings. It then distinguishes the contribution that can reasonably be claimed from the limitations that constrain generalization and causal interpretation. The section concludes by identifying concrete directions for instrument refinement, stronger research designs, broader sampling, and comparative studies that can test and extend the privacy-trust-engagement mechanism identified in the present research.

This study investigated whether perceived trust mediates the relationship between data privacy concern and consumer engagement with global digital platforms in Bangladesh. Using 385 complete attention-check-passing cases, the analysis found that privacy concern was positively associated with trust, trust was positively associated with engagement, and the small total privacy concern-engagement association became non-significant after trust was included. Bootstrap analysis identified a statistically detectable indirect effect through trust. The results therefore suggest that privacy concern and engagement can coexist and that trust is an important relational mechanism in this coexistence.

The contribution is threefold. Substantively, the study provides Bangladesh evidence on privacy, trust and engagement across global platform ecosystems. Theoretically, it integrates Privacy Calculus Theory with Trust Theory to foreground an indirect trust mechanism rather than assuming a simple privacy-risk withdrawal effect. Methodologically, it demonstrates transparent handling of an imperfect field instrument: significant structural relationships are reported alongside weak reliability and item-overlap concerns rather than being presented as unqualified SEM evidence.

The limitations are material. The cross-sectional design prevents causal inference and temporal mediation claims. Purposive sampling limits population generalizability. All focal variables are self-reported, creating potential common-method bias. Most importantly, Cronbach's alpha values for the focal three-item scales are below conventional confirmatory thresholds, and some item wording creates conceptual overlap between privacy concern, trust and engagement. PC3 partly measures a consequence of concern rather than concern itself. The engagement items also condition behavior on trust/privacy expectations. These measurement limitations warrant cautious interpretation of the observed relationships and preclude treating the current measurement model as fully validated.

Future research should redevelop the instrument before a new field wave. Privacy concern can be measured with validated IUIPC-style dimensions; trust should distinguish ability, integrity and benevolence or platform-specific reliability; engagement should use behaviorally clean cognitive, affective and behavioral dimensions. A pilot CFA should precede full data collection. Subsequent studies could use longitudinal designs to establish temporal order,

experiments manipulating privacy transparency, objective platform-use indicators, and probability or stratified sampling. Multi-group analysis could examine whether the mechanism differs by AI experience, age, gender, platform category or digital literacy. Cross-country comparison with other South Asian emerging economies would further test contextual boundary conditions.

Declarations

Ethics approval: This non-clinical, minimal-risk study was undertaken as part of an academic field exercise. No dedicated institutional ethics review mechanism or formal ethics approval number was available for this course-based research within the researchers' institutional setting at the time of data collection. Nevertheless, internationally recognized ethical principles for research involving human participants were followed, including voluntary participation, informed consent, anonymity, confidentiality, and protection of participant privacy.

Informed consent: Participants were required to indicate consent before participation.

Data availability: The anonymized research dataset is held by the research team and supervisor and may be made available subject to applicable ethical and institutional restrictions.

Conflict of interest: The authors declare no conflict of interest.

Funding: This research received no external funding.

Author contributions: Mst. Tahsina Jannat: Conceptualization, investigation, data collection, data curation, literature review, formal analysis, and writing – original draft. Atifa Akter Juthy: Investigation, literature

review, data validation, interpretation of findings, and writing – review and editing. Sraboni Akter: Investigation, data verification, literature review, interpretation of results, and writing – review and editing. Prof. Dr Kazi Abdul Mannan: Conceptualization, methodology, research design, supervision, formal analysis, validation, interpretation of findings, manuscript development, and writing – review and editing. All authors critically reviewed the manuscript, approved the final version for publication, and agreed to be accountable for their respective contributions to the work..

AI disclosure: Any use of generative-AI tools in the preparation of this manuscript must be disclosed in accordance with the policy of the journal selected for submission. The authors retain full responsibility for verification, analysis, interpretation, and the final manuscript.

References

- [1] T. Fernandes and N. Pereira, “Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online?,” *Telematics and Informatics*, vol. 65, 101717, 2021. doi:10.1016/j.tele.2021.101717.
- [2] F. T. Beke, F. Eggers, P. C. Verhoef, and J. E. Wieringa, “Consumers’ privacy calculus: The PRICAL index development and validation,” *International Journal of Research in Marketing*, vol. 39, no. 1, pp. 20-41, 2022. doi:10.1016/j.ijresmar.2021.05.005.
- [3] L. F. Bright et al., “Should I Post or Ghost? Examining how privacy concerns impact social media engagement in US consumers,” *Psychology & Marketing*, 2021. doi:10.1002/mar.21499.
- [4] S. Kim, “Privacy concerns and digital engagement: Evidence from a national panel survey,” *Information Economics and Policy*, vol. 73, 101164, 2026. doi:10.1016/j.infoecopol.2026.101164.
- [5] A. Acquisti, C. Taylor, and L. Wagman, “The economics of privacy,” *Journal of Economic Literature*, vol. 54, no. 2, pp. 442-492, 2016.
- [6] M. J. Culnan and P. K. Armstrong, “Information privacy concerns, procedural fairness, and impersonal trust,” *Organization Science*, vol. 10, no. 1, pp. 104-115, 1999.
- [7] Bangladesh Telecommunication Regulatory Commission, “Internet Subscribers,” 2026.
- [8] Bangladesh Telecommunication Regulatory Commission, “Teledensity and Penetration,” 2026.
- [9] F. Hossain, M. R. Islam, and S. Zaman, “Exploring the Digital Financial Service in Bangladesh: Unraveling the Dynamics of Trust, Fear, and Privacy,” *Annals of Anthropological Practice*, vol. 49, no. 2, e70018, 2025. doi:10.1111/napa.70018.
- [10] M. F. Rabbi and A. C. Roy, “Personal data security in online tax filing systems in Bangladesh: Trust, concerns, and adoption barriers,” *Social Sciences & Humanities Open*, vol. 13, 103055, 2026. doi:10.1016/j.ssaho.2026.103055.
- [11] T. Dinev and P. Hart, “An extended privacy calculus model for e-commerce transactions,” *Information Systems Research*, vol. 17, no. 1, pp. 61-80, 2006.
- [12] R. E. Goldsmith and E. Horowitz, “Measuring motivations for online opinion

- seeking,” *Journal of Interactive Advertising*, 2006.
- [13] “The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO,” *Computers & Security*, vol. 126, 103071, 2023. doi:10.1016/j.cose.2022.103071.
- [14] J. L. Hayes, N. H. Brinson, G. J. Bott, and C. M. Moeller, “The Influence of Consumer-Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media,” *Journal of Interactive Marketing*, vol. 55, no. 1, 2022. doi:10.1016/j.intmar.2021.01.001.
- [15] R. J. Brodie et al., “Consumer engagement in a virtual brand community: An exploratory analysis,” *Journal of Business Research*, vol. 66, no. 1, pp. 105-114, 2013.
- [16] I. J. Shithii, A. Al-Jahan, and M. A. H. Mia, “Consumer Trust and Privacy Concerns in AI-Driven E-Commerce: Evidence from a Hybrid SEM-ANN Study,” *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 21, no. 7, 228, 2026. doi:10.3390/jtaer21070228.
- [17] H. J. Smith, S. J. Milberg, and S. J. Burke, “Information privacy: Measuring individuals’ concerns about organizational practices,” *MIS Quarterly*, vol. 20, no. 2, pp. 167-196, 1996.
- [18] N. K. Malhotra, S. S. Kim, and J. Agarwal, “Internet Users’ Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model,” *Information Systems Research*, vol. 15, no. 4, pp. 336-355, 2004.
- [19] M. J. Culnan and R. J. Bies, “Consumer privacy: Balancing economic and justice considerations,” *Journal of Social Issues*, vol. 59, no. 2, pp. 323-342, 2003.
- [20] R. C. Mayer, J. H. Davis, and F. D. Schoorman, “An integrative model of organizational trust,” *Academy of Management Review*, vol. 20, no. 3, pp. 709-734, 1995.
- [21] D. H. McKnight, V. Choudhury, and C. Kacmar, “Developing and validating trust measures for e-commerce,” *Information Systems Research*, vol. 13, no. 3, pp. 334-359, 2002.
- [22] P. A. Pavlou, “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model,” *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101-134, 2003.
- [23] D. Gefen, E. Karahanna, and D. W. Straub, “Trust and TAM in online shopping: An integrated model,” *MIS Quarterly*, vol. 27, no. 1, pp. 51-90, 2003.
- [24] S. D. Vivek, S. E. Beatty, and R. M. Morgan, “Customer engagement: Exploring customer relationships beyond purchase,” *Journal of Marketing Theory and Practice*, vol. 20, no. 2, pp. 122-146, 2012.
- [25] L. D. Hollebeek, M. S. Glynn, and R. J. Brodie, “Consumer brand engagement in social media,” *Journal of Interactive Marketing*, vol. 28, no. 2, pp. 149-165, 2014.
- [26] J. van Doorn et al., “Customer engagement behavior: Theoretical foundations and research directions,” *Journal of Service Research*, vol. 13, no. 3, pp. 253-266, 2010.
- [27] V. Kumar et al., “Undervalued or overvalued customers: Capturing total customer engagement value,” *Journal of Service Research*, vol. 13, no. 3, pp. 297-310, 2010.

- [28] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122-134, 2017.
- [29] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are privacy concerns a turn-off? Engagement and privacy in social networks," *SOUPS*, 2012.
- [30] M. Daradkeh, "Privacy policies and user self-disclosure in social media: the mediating effect of social media trust," *International Journal of Business Innovation and Research*, vol. 38, no. 2, pp. 221-239, 2025.
- [31] H. Brits and N. Jonker, "The Use of Financial Apps: Privacy Paradox or Privacy Calculus?," *De Nederlandsche Bank Working Paper 794*, 2023.
- [32] "Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory," *Decision Support Systems*, vol. 165, 113881, 2023. doi:10.1016/j.dss.2022.113881.
- [33] L. Zhu et al., "Do people disclose less after experiencing privacy invasion? The moderating role of digital privacy literacy and gender differences," *Acta Psychologica*, vol. 267, 107022, 2026. doi:10.1016/j.actpsy.2026.107022.
- [34] J. F. Hair Jr. et al., *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed. Sage, 2022.
- [35] J. F. Hair et al., "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2-24, 2019.
- [36] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, 1981.
- [37] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, vol. 43, pp. 115-135, 2015.
- [38] J. C. Nunnally and I. H. Bernstein, *Psychometric Theory*, 3rd ed. McGraw-Hill, 1994.
- [39] A. F. Hayes, *Introduction to Mediation, Moderation, and Conditional Process Analysis*, 3rd ed. Guilford Press, 2022.
- [40] C. M. Judd and D. A. Kenny, "Process analysis: Estimating mediation in treatment evaluations," *Evaluation Review*, vol. 5, pp. 602-619, 1981.

Appendix A. Focal Measurement Items

The appendix reproduces the nine focal questionnaire items used to construct the three composite variables analyzed in this article. Presenting the exact wording allows readers to evaluate construct coverage and the measurement limitations discussed in Sections 3, 4 and 7.

Table A1. Focal Constructs and Measurement Items

Construct	Code	Item
Privacy Concern	PC1	I am concerned about how global digital platforms collect my personal information.
Privacy Concern	PC2	I worry about secondary uses of my data that I may not fully understand.
Privacy Concern	PC3	Privacy concerns affect how actively I engage with digital platforms.
Perceived Trust	TR1	I trust reputable global technology platforms to provide reliable services.
Perceived Trust	TR2	I believe responsible platforms should handle user data with care.
Perceived Trust	TR3	I feel confident relying on established global digital platforms for important activities.
Consumer Engagement	CE1	I interact actively with digital platforms that I trust.
Consumer Engagement	CE2	I spend more time using platforms that provide valuable and trustworthy experiences.
Consumer Engagement	CE3	I am willing to participate more deeply in services when privacy and trust expectations are met.