Journal link: http://kmf-publishers.com/tatscr/

Theoretical and Applied Technological Science Review

Volume: 4 Issue: 4 Year: 2026
ISSN-2958-7824



KMF PUBLISHERS

www.kmf-publishers.com/tatscr/

Received: 20 September 2026 | Revised: 25 October 2026 | Accepted: 28 October 2026

DOI: https://doi.org/10.64907/xkmf.v4i4.tatscr.3

Published: 30 October 2026

Research Article

Privacy Concern and Conditional Willingness to Adopt AI Legal Platforms in Bangladesh

Farhan Islam[1*]; Moumita Akter Mira[1]; Sumaiya Akter[1]; Kazi Abdul Mannan[2]

[1]Department of Law
[2]Department of Business Administration
Shanto-Mariam University of Creative Technology
Dhaka, Bangladesh

*Correspondence
Farhan Islam
Email: shoumikahmedfarhan@gmail.com

ABSTRACT

Privacy concerns may discourage the use of artificial intelligence in legal services while also motivating interest in platforms with credible safeguards. These responses are often collapsed into a single adoption construct, obscuring whether respondents reject the technology or condition its use on protection. This study examines that distinction in 385 adult, AI-aware survey records from Bangladesh, including 242 law students. Five statements separately measure disclosure concern, self-attributed inhibition, conditional willingness under strong privacy controls, preference for meaningful data control, and the perceived influence of trust. Analyses combine joint response patterns, paired endorsement contrasts, ordinal correlations and exploratory logistic models with robust covariance estimates. Disclosure concern was endorsed by 56.1%, privacy-related inhibition by 75.6%, conditional willingness under strong controls by 72.7%, meaningful-control preference by 53.2%, and the influence of trust by 79.0%. Inhibition and conditional willingness coexisted in 216 records (56.1%). Concern had a small positive ordinal association with conditional willingness ($\rho = 0.149$; Holm-adjusted $p = 0.013$), but its adjusted association with binary endorsement was uncertain (odds ratio 1.29; 95% interval 0.98-1.69). None of the four focal adjusted model tests met the 0.05 threshold after Holm correction. The findings identify conditional acceptance within the recorded sample, rather than an observed privacy paradox or an effect on actual adoption. The article contributes a distinction between concern, attributed inhibition and safeguard-contingent willingness. It recommends evaluating concrete privacy controls through tasks that measure informed choices, alongside technical protection. Undocumented recruitment and fieldwork dates constrain population inference and temporal interpretation.

Keywords: privacy calculus; legal technology; data control; conditional acceptance; information privacy; Bangladesh

Copyright: 2026 by the authors. Licensee KMF Publishers (www.kmf-publishers.com). This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

An AI legal platform can help a person search for information, organise documents or formulate an initial question. The same interaction may require details about an employment dispute, family relationship, financial position or allegation of wrongdoing. Adoption therefore involves more than confidence in an answer. Users also need to understand what information leaves their control, who may access it and whether the service can perform the task with less sensitive input. These questions become especially consequential where a user describes another person's circumstances or a lawyer handles information entrusted by a client. Comparative professional guidance addresses confidentiality alongside competence and communication when lawyers use generative AI.[1]

Privacy risk is technically plausible, although its form depends on the system and deployment. Research has demonstrated extraction of training examples from a language model and inference of personal attributes from text in separate experimental settings. These findings identify different routes to exposure; they do not establish that every legal platform leaks confidential information.[2] A useful adoption analysis must therefore distinguish a respondent's concern about possible disclosure from a measured security defect. It must also distinguish a preference for protection from evidence that protection has been implemented.

Bangladesh provides the setting for the present survey. Article 43 of its Constitution includes protection of correspondence and other means of communication, subject to specified restrictions.[3] The legal context has also changed through the Personal Data Protection Act 2026. That Act replaced the 2025 ordinance and its 2026 amendment, with commencement provisions that require attention to the particular section.[4] These legal developments provide context for discussing privacy, but the questionnaire does not test knowledge of this legislation. Because fieldwork dates are undocumented, the analysis cannot identify respondents' exposure to any particular legal regime.

The research problem is how perceived privacy risk relates to willingness to use AI legal services when the available statements incorporate different conditions. A respondent can worry about exposure, report that privacy concerns reduce willingness for sensitive matters, and still prefer a platform with strong safeguards. Such answers need not conflict. They can describe the same

[1] American Bar Association Standing Committee on Ethics and Professional Responsibility, ‘Generative Artificial Intelligence Tools’ (Formal Opinion 512, 29 July 2024).

[2] Nicholas Carlini and others, ‘Extracting Training Data from Large Language Models’ in 30th USENIX Security Symposium (USENIX Association 2021) 2633; Robin Staab and others, ‘Beyond Memorization: Violating Privacy via Inference with Large Language Models’ in The Twelfth International Conference on Learning Representations (2024) <https://proceedings.iclr.cc/paper_files/paper/2024/hash/9028b8a3ca98f58e373f0c1497a17448-Abstract-Conference.html> accessed 28 October 2026.

[3] The Constitution of the People’s Republic of Bangladesh, art 43.

[4] Personal Data Protection Act 2026 (Bangladesh) (Act No 63 of 2026), ss 1 and 44 <https://bdlaws.minlaw.gov.bd/act-details-1692.html> accessed 28 October 2026.

decision under different assumptions about protection. Treating every statement as an interchangeable indicator of acceptance could conceal this distinction and produce a model whose apparent precision exceeds its conceptual clarity.

Privacy-calculus research examines competing considerations in decisions to disclose information. It provides a basis for asking whether concern and conditional willingness coexist, rather than assuming a uniformly negative relationship.[5] Yet an item saying that privacy concerns reduce willingness already contains a proposed explanatory relationship. Agreement with that sentence cannot independently estimate how much concern changes adoption. Similarly, agreement that trust affects intention does not measure an actual level of trust or the direction and size of its effect. These measurement issues matter before any regression or structural model is fitted.

The supplied questionnaire contains no record of registration for a legal platform, transaction completion or abandonment. It also lacks a separately worded unconditional adoption-intention measure. Accordingly, this article examines conditional willingness and related response patterns. It retains the substantive question about risk and adoption while narrowing the empirical claims to outcomes that the instrument can support.

Information-privacy scholarship differentiates concerns about collection, awareness and control, and has examined how privacy relates to trust and disclosure.[6] Recent syntheses continue to identify variation across contexts and relationships.[7] This study contributes a precise empirical specification of a legal-service decision: whether concern, reported inhibition and interest in protected use appear together in the same records, and whether their associations depend on the response being analysed. The study does not claim that this distinction is absent from all previous research or that the sample represents Bangladesh nationally.

The article makes three connected contributions. First, it uses the content of the five focal statements to separate a concern judgement from self-attributed inhibition, conditional willingness, a control preference and an attribution to trust. Second, it compares joint patterns with both ordinal and binary analyses. This reveals whether a broad ranking relationship translates into a distinction at an agreement threshold. Third, it connects these results to a practical evaluation problem: a platform should demonstrate the effectiveness and usability of safeguards rather than interpret stated willingness as permission for unrestricted data collection. That final proposition draws

[5] Tamara Dinev and Paul Hart, ‘An Extended Privacy Calculus Model for E-Commerce Transactions’ (2006) 17 Information Systems Research 61.

[6] Naresh K Malhotra, Sung S Kim and James Agarwal, ‘Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model’ (2004) 15 Information Systems Research 336; H Jeff Smith, Tamara Dinev and Heng Xu, ‘Information Privacy Research: An Interdisciplinary Review’ (2011) 35 MIS Quarterly 989.

[7] Truong (Jack) Luu and Andrew Harrison, ‘Understanding Information Privacy Concerns: A Meta-Analytic of Three Decades of Research’ (2026) Information Systems Research, advance online publication, doi:10.1287/isre.2023.0797; Christian Herriger and others, ‘Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, Augmented Reality, Big Data, and the Internet of Things: Systematic Review’ (2025) 27 Journal of Medical Internet Research e71951.

on privacy-risk management and remains a recommendation for evaluation.[8]

The general objective is to examine privacy-related conditions of potential AI legal-platform use in the recorded Bangladesh sample. The analysis asks four questions. How are responses distributed across the five focal statements? To what extent do disclosure concern and self-attributed inhibition coexist with willingness under strong privacy controls? How do ordinal associations compare with adjusted associations at an endorsement threshold? How sensitive are the descriptions to law-student restriction and alternative concern coding?

These questions organise an exploratory analysis, rather than preregistered confirmatory tests. Section 2 establishes the theoretical distinctions and analytical expectations. Section 3 describes the records and methods. Results are reported in Section 4 and interpreted in Section 5. Sections 6 and 7 develop implications, limitations and a research agenda. Declarations specify ethical safeguards, author responsibilities and AI assistance.

2. Literature Review and Theoretical Foundation

Privacy calculus provides the principal theoretical lens. Protection motivation and planned behaviour clarify why concern, safeguards and intention should be measured separately. Contextual integrity connects those individual judgements to the conditions under which legal information moves. The frameworks guide interpretation; the survey does not operationalise all their constructs or permit a comprehensive test of any one theory.

2.1 Privacy concern and the object of adoption

Perceived privacy risk concerns possible adverse consequences of collecting, processing or disclosing information. The present concern item is narrower: worry that an AI legal platform may expose personal or confidential information. It does not separately measure probability, severity or prior experience of harm. This specificity is useful because it identifies the feared event, but it limits the breadth of the resulting construct. Multidimensional privacy instruments should not be assumed to have been reproduced by a single locally supplied statement.[9]

Adoption also requires definition. Actual use, willingness to register, intention to share a document and willingness to use a protected service are different outcomes. The present PPR3 statement asks whether a person would be more willing if a platform offered strong privacy controls. Its

[8] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (version 1.0, 2020).
[9] Malhotra, Kim and Agarwal (n 6).

comparative wording supplies a protective condition without specifying a baseline willingness. A respondent can endorse it while remaining unwilling in absolute terms. PPR4 instead asks about preferring meaningful control over personal data. A preference between services may be strong even where neither service is ultimately used.

This separation avoids interpreting an answer as more than it records. The survey offers information about conditions respondents consider relevant, not a market forecast. Nor does the reference to legal platforms demonstrate familiarity with a named product. Participants were screened for general AI awareness, and reported tool exposure concerns AI broadly. The article therefore discusses potential acceptance of legal services among AI-aware respondents rather than adoption among a verified cohort of legal-platform customers.

2.2 Privacy calculus as the primary lens

Dinev and Hart's extended privacy-calculus model treats disclosure as a decision involving both inhibiting considerations and factors that can encourage a transaction. Their e-commerce research examined concerns, trust and other motivations in a structured model.[10] Its relevance here is the possibility of simultaneous restraint and conditional engagement. Privacy concern can make a person reluctant to submit sensitive material while increasing the value placed on safeguards. A negative attitude toward exposure need not imply rejection of every form of AI assistance.

The current study cannot estimate a full calculus. It contains no distinct benefit scale, monetary trade-off or task-specific valuation, and the trust item concerns the perceived influence of protection rather than trust itself. Consequently, a positive association between concern and safeguard-contingent willingness would be compatible with a calculus interpretation without demonstrating that respondents consciously balanced benefits against expected loss. The same pattern could reflect response style, general favourability toward safeguards or unmeasured experience.

An important implication is that a total PPR score would lack a straightforward meaning. More concern, more inhibition and stronger preference for protection do not all move acceptance in the same direction. Reverse-scoring inhibition would not solve the problem: it would impose a continuum in

[10] Dinev and Hart (n 5).

which endorsement of protections must imply acceptance. We instead preserve the separate response objects and investigate their empirical relationships. This strategy allows a theoretically meaningful question even when the available instrument cannot support a latent causal model.

2.3 Protection motivation and coping conditions

Protection-motivation theory differentiates appraisals of threat from appraisals of coping, including response efficacy and self-efficacy. Maddux and Rogers tested these distinctions in experimental work on fear appeals.[11] In information security, Johnston and Warkentin examined how fear appeals relate to intentions to follow protective recommendations, with differences across users.[12] These contributions motivate a practical distinction between recognising a potential threat and believing that a particular response can manage it.

PPR1 resembles a threat-related concern. PPR3 mentions a protective condition, but it does not ask whether respondents believe the controls work or whether they can operate them. PPR4 values meaningful control without measuring task performance. These are partial conceptual connections, not validated substitutes for response efficacy or self-efficacy. The study therefore avoids claiming that protection motivation mediates any observed relationship. A future test would need separate measures and a defined protective action, such as withholding a sensitive document or changing a retention setting.

2.4 Planned behaviour and the limits of attributed intention

The theory of planned behaviour relates intention to attitudes, subjective norms and perceived behavioural control, with behaviour also depending on opportunities and control.[13] This perspective requires a clearly specified action. Willingness to obtain general legal information is not equivalent to willingness to upload a confidential case file. The instrument refers to sensitive legal matters in PPR2, an AI platform in PPR3 and a legal platform in PPR4. Those changes in referent can affect answers even when every statement uses the same agreement scale.

PPR2 says that privacy concerns reduce willingness. PPR5 says that trust in data protection affects adoption intention. Both statements attribute influence within their wording. They can reveal respondents' beliefs about the relevance of privacy, but they cannot serve simultaneously as independent evidence of the proposed mechanisms. The present model accordingly uses PPR2 as a reported inhibition judgement and labels it throughout. It does not reconstruct an unmeasured baseline intention by reversing the response. Subjective norms and perceived behavioural

[11] James E Maddux and Ronald W Rogers, ‘Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change’ (1983) 19 Journal of Experimental Social Psychology 469.
[12] Allen C Johnston and Merrill Warkentin, ‘Fear Appeals and Information Security Behaviors: An Empirical Study’ (2010) 34 MIS Quarterly 549.
[13] Icek Ajzen, ‘The Theory of Planned Behavior’ (1991) 50 Organizational Behavior and Human Decision Processes 179.

control were not separately measured, so planned behaviour functions as a guide to future measurement rather than a theory declared confirmed.

2.5 Control and credible assurance

Control can mean deciding what to disclose, choosing who receives it or limiting subsequent processing. These capabilities are related but operationally different. Brandimarte, Acquisti and Loewenstein's experiments show why greater perceived control should not automatically be equated with lower exposure: changes in control can also change willingness to disclose.[14] The implication for legal platforms is to evaluate both what a control actually prevents and how users interpret its protection.

Research on privacy assurance mechanisms further distinguishes the presentation of safeguards from the formation of trust, while work on context and personality emphasises that disclosure decisions depend on circumstances.[15] The two current safeguard items can therefore be compared descriptively without assuming measurement equivalence. “Strong privacy controls” may evoke general protection, whereas “meaningful control over personal data” may evoke individual agency. Their different endorsement rates cannot identify which interpretation respondents used. Interviews and controlled wording experiments would be required to distinguish those possibilities.

2.6 Contextual integrity and legal confidentiality

Contextual integrity evaluates information flows in relation to their context, participants and transmission conditions.[16] It is especially useful for legal services, where the person typing information may not be its only subject. A user may be authorised to seek advice yet lack authority to make unrestricted secondary disclosure about a relative, opposing party or client. Protection consequently involves more than allowing the immediate user to click a consent box.

Technical studies on language models also make it necessary to distinguish routes of exposure. Memorised training material and inference from new text present different problems, even if users describe both as a loss of privacy.[17] A provider's explanation should identify the relevant information flow and safeguard rather than rely on a generic claim that AI is secure. NIST's generative-AI profile treats privacy within a broader risk-management approach, offering a reference for systematic evaluation.[18] None of these technical risks is measured directly in the present questionnaire.

[14] Laura Brandimarte, Alessandro Acquisti and George Loewenstein, ‘Misplaced Confidences: Privacy and the Control Paradox’ (2013) 4 Social Psychological and Personality Science 340.

[15] Gaurav Bansal, Fatemeh Mariam Zahedi and David Gefen, ‘The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern’ (2015) 24 European Journal of Information Systems 624; Gaurav Bansal, Fatemeh Mariam Zahedi and David Gefen, ‘Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online’ (2016) 53 Information & Management 1.

[16] Helen Nissenbaum, ‘Privacy as Contextual Integrity’ (2004) 79 Washington Law Review 119.

[17] Carlini and others (n 2); Staab and others (n 2).

[18] Chloe Autio and others, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1, National Institute of Standards and Technology 2024).

2.7 Evidence on concern and behaviour

The privacy-paradox literature examines apparent discrepancies between expressed concern and behaviour, but the inference depends on how both are observed. Solove challenges reasoning that treats a particular disclosure as evidence that people do not value privacy.[19] Baruh, Seçinti and Cemalcılar's meta-analysis distinguishes service use, information sharing and privacy management.[20] These contributions support matching the level of concern to the particular decision under study.

The present survey contains stated preferences and self-attributions rather than observed disclosure. Its joint response patterns therefore cannot establish a privacy paradox. Privacy fatigue is another possible account of disengagement, but it also requires evidence beyond a concern item.[21] The study does not diagnose resignation, inconsistency or lack of care from neutral answers. Recent syntheses by Herriger and colleagues and by Luu and Harrison reinforce the value of examining context and differentiated relationships instead of assuming a single general concern effect.[22]

2.8 Analytical expectations and framework

The analysis develops two expectations for exploration. First, reported inhibition and conditional willingness may coexist because they refer to use under different privacy conditions. Second, concern may be positively associated with valuing safeguards, while its association with a general control preference may differ. Neither expectation requires a negative relationship between every privacy item and acceptance. The analyses were selected for this article after the available instrument was inspected; they are not presented as preregistered hypotheses.

Figure 1 maps the measured objects and identifies the outcomes that remain outside the dataset. The exploratory logistic specifications compare endorsement of PPR3 and PPR4 separately, using concern and reported inhibition with limited AI-experience and status covariates. PPR5 is described separately because attribution to trust cannot substitute for an independently measured trust construct. The framework creates an explicit boundary between an estimated association among questionnaire responses and a causal claim about actual platform use.

[19] Daniel J Solove, ‘The Myth of the Privacy Paradox’ (2021) 89 George Washington Law Review 1.

[20] Lemi Baruh, Ekin Seçinti and Zeynep Cemalcılar, ‘Online Privacy Concerns and Privacy Management: A Meta-Analytical Review’ (2017) 67 Journal of Communication 26.

[21] Hanbyul Choi, Jonghwa Park and Yoonhyuk Jung, ‘The Role of Privacy Fatigue in Online Privacy Behavior’ (2018) 81 Computers in Human Behavior 42.

[22] Herriger and others (n 7); Luu and Harrison (n 7).

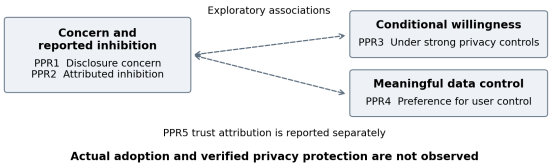

Figure 1. Framework for analysing privacy judgements and conditional acceptance

Dashed connections identify exploratory associations. Models adjust for AI-use frequency, training and law-student status. No arrow denotes an estimated causal effect or a pathway to actual adoption.

3. Methodology

The study uses a quantitative cross-sectional design to analyse the privacy-risk and adoption block of the Group 5 survey. The reporting distinguishes available records, the research plan and researcher-confirmed ethical arrangements. A design preference in a proposal is not treated as evidence that the procedure occurred. This distinction follows the transparency objective of observational reporting guidance.[23]

3.1 Population and analytical sample

The workbook contains 385 records. Every record includes affirmative consent, adult eligibility and relevant AI awareness. The unit of analysis is an individual recorded questionnaire response. Current status identifies 242 law students, 71 law graduates, 42 advocates or legal professionals, and 30 other relevant respondents. Eligibility is therefore broader than practising legal professionals, and current legal-platform use is not established. The analysis retains this mixed sample and separately describes the recorded student and non-student subsets.

The database is supplied by the researchers as real survey data. Its Codebook describes the respondent sequence as synthetic and the optional contextual comments as synthetic text. Those labels do not establish that the numerical answers are simulated; they do create a need to document how identifiers and comments relate to source records. The analysis excludes comments entirely and uses the sequence solely to distinguish rows. Original questionnaires and recruitment documentation remain necessary for source verification.

[23] Erik von Elm and others, ‘The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies’ (2007) 4 PLOS Medicine e296.

3.2 Sampling and sample size

The plan targets 385 completed questionnaires for a large or unknown population. Cochran's conventional calculation with Z = 1.96, p = 0.50 and e = 0.05 gives 384.16, rounded upward.[24] That rationale explains the planned count under simple-random-sampling assumptions. It does not establish a national sampling frame, actual random selection or a population margin of error for the supplied records. The plan's preferred probability approach and anticipated contact allowance are not reported as completed field procedures.

The materials do not document actual fieldwork dates, institutions, recruitment channels, numbers invited or exclusions preceding the workbook. A response rate cannot be calculated. All 385 available records enter the focal analysis; this is a final analytical count rather than proof that every approached respondent participated. No survey weights are applied because selection probabilities are unavailable. Confidence intervals describe uncertainty under conventional model or resampling assumptions and cannot compensate for an undocumented selection process.

3.3 Instrument and measurement specification

Five PPR statements use ordered responses from 1, strongly disagree, to 5, strongly agree. Table 1 sets out their meanings and empirical roles. Their source is the supplied questionnaire and matching Codebook. An item-level adaptation record is unavailable, so the statements are identified as study-specific rather than as reproductions of a validated scale. Theoretical sources provide conceptual support for their interpretation.

Table 1. Focal statements and analytical interpretation

Item	Statement focus	Analytical interpretation
PPR1	Worry about exposure of personal or confidential information	Disclosure concern; not measured breach risk
PPR2	Privacy concerns reduce willingness for sensitive legal matters	Self-attributed inhibition; not a separately estimated effect
PPR3	Greater willingness under strong privacy controls	Conditional willingness; not baseline or actual adoption
PPR4	Preference for meaningful control over personal data	Control preference; not tested ability to use controls
PPR5	Trust in data protection affects adoption intention	Attribution to trust; not measured trust level

Source: Group 5 questionnaire and Codebook; exact wording in Appendix A.

The statements cover different objects, including an emotion, attributed inhibition, conditional willingness, a preference and a belief about influence. They are analysed separately. Preliminary coefficient alpha for the five-item block is 0.183, but the substantive argument against aggregation arises first from the wording. Alpha does not

[24] William G Cochran, Sampling Techniques (3rd edn, John Wiley & Sons 1977).

establish unidimensionality or construct validity, and deleting items solely to raise it would not create a valid adoption scale.[25] No latent path model, mediation model, composite reliability, average variance extracted or HTMT estimate is reported for these heterogeneous statements.

3.4 Screening and documentation

There are no missing values in PPR1-PPR5 or in the model covariates. Nine records lack the optional AI-tool response, which is not included in the models. Identifiers are unique and no exact duplicate is found after excluding the identifier and contextual-text field. Eleven respondents provide the same answer across the five focal statements, but none gives one constant response across all 20 Likert items. These observations do not independently verify respondents' identities or attention.

The questionnaire contains a self-rated understanding item but no objectively scored attention check. Completion times, recruitment logs and platform-use verification are absent. Constant focal responses are retained because agreement across five related statements can be substantive. No imputation, data-driven deletion or weighting is performed. A separate pilot sample, translation procedure, cognitive interview record and item-revision history are not documented; none is inferred from the general instrument protocol.

3.5 Descriptive and joint response analyses

All five response-category counts, means and standard deviations are reported. Means serve as descriptive summaries, while ordinal correlations avoid assuming equally spaced categories. Endorsement combines agree and strongly agree. Wilson intervals accompany endorsement proportions.[26] Neutral answers remain visible and are grouped with disagreement only for the binary endorsement analyses; non-endorsement is not described as opposition.

Two cross-tabulations examine concern with conditional willingness and reported inhibition with conditional willingness. Each partitions the same 385 records into both endorsed, first only, second only and neither. These are response combinations, not latent user types. Two paired contrasts compare PPR3 with PPR4 and PPR2 with PPR1. Exact McNemar tests use discordant pairs, with Holm correction within this two-test family.[27] Pointwise percentile intervals for the endorsement differences use 10,000 whole-respondent bootstrap resamples.[28]

[25] Klaas Sijtsma, ‘On the Use, the Misuse, and the Very Limited Usefulness of Cronbach’s Alpha’ (2009) 74 Psychometrika 107.

[26] Edwin B Wilson, ‘Probable Inference, the Law of Succession, and Statistical Inference’ (1927) 22 Journal of the American Statistical Association 209.

[27] Quinn McNemar, ‘Note on the Sampling Error of the Difference between Correlated Proportions or Percentages’ (1947) 12 Psychometrika 153; Sture Holm, ‘A Simple Sequentially Rejective Multiple Test Procedure’ (1979) 6 Scandinavian Journal of Statistics 65.

[28] Bradley Efron and Robert J Tibshirani, An Introduction to the Bootstrap (Chapman & Hall 1993).

3.6 Ordinal and adjusted association analyses

Four Spearman correlations compare concern, PPR1, with each other focal statement. Pointwise percentile intervals use 4,000 respondent bootstrap resamples. Holm adjustment covers these four exploratory tests as a separate family. The correlations describe ranks among responses and are not interpreted as changes caused by concern.

Two binary logistic models estimate endorsement of PPR3 and PPR4 separately. Each contains PPR1 concern and PPR2 reported inhibition as one-point ordinal predictors, weekly-or-more AI use versus less frequent use, any formal AI training versus none, and law-student status versus other statuses. These covariates describe exposure and sample composition; they do not form a sufficient causal adjustment set. Estimates are adjusted odds ratios with heteroskedasticity-robust sandwich intervals. Logistic modelling provides a compact conditional association at the stated response threshold.[29]

The four focal coefficients, concern and inhibition across two outcomes, receive Holm correction as one family. Covariate intervals are descriptive. The three families address different questions and do not constitute a single article-wide correction. Exploratory interpretation remains necessary. Sensitivity analyses separate students from non-students, replace linear concern scoring with category indicators, and tabulate strong agreement. Models do not estimate actual adoption or clinical-style individual prediction. Data preparation and statistics were implemented programmatically in Python using pandas, NumPy, SciPy and statsmodels.

3.7 Ethical considerations

Formal approval was not obtained because the authors' institutional setting lacked an accessible formal review mechanism applicable to this non-interventional adult questionnaire research. The researchers confirm that consent preceded participation and that participation was voluntary, anonymous and discontinuable. The questionnaire explains the academic purpose, states that names are unnecessary and promises aggregate analysis. All retained records contain affirmative consent and adult eligibility. Contextual text is excluded, and reporting avoids individual disclosures.

4. Results

Results distinguish distributions, coexisting responses and estimated associations. Percentages refer to the 385 available records unless another denominator is stated. The analyses concern reported judgements about privacy and potential use, with no observed platform registration, document disclosure or adoption event.

[29] David W Hosmer Jr, Stanley Lemeshow and Rodney X Sturdivant, Applied Logistic Regression (3rd edn, John Wiley & Sons 2013); Halbert White, ‘A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity’ (1980) 48 Econometrica 817.

4.1 Respondent profile and data completeness

Table 2 describes sample composition and exposure variables relevant to interpretation. Law students comprise the largest recorded status group, but the sample includes graduates and professionals. This composition is retained in the main analysis and addressed through status adjustment and subset summaries.

Table 2. Respondent status and AI experience

Measure	Category	Count (%)
Status	Law student	242 (62.9%)
	Law graduate	71 (18.4%)
	Advocate or legal professional	42 (10.9%)
	Other relevant respondent	30 (7.8%)
AI-use frequency	Weekly	154 (40.0%)
	Daily or almost daily	121 (31.4%)
	Monthly	64 (16.6%)
	Less than monthly	31 (8.1%)
	Never	15 (3.9%)
AI training	No	225 (58.4%)
	Yes, short orientation	106 (27.5%)
	Yes, course or certified training	54 (14.0%)

N = 385. Status and AI experience are recorded categories, without confirmation of named legal-platform use. Additional age, gender and location summaries are reported in the accompanying text.

Law students account for 62.9% of records. The largest age category is 21-23 years, with 163 respondents (42.3%), followed by 24-26 years with 81 (21.0%). There are 200 male respondents (51.9%), 173 female respondents (44.9%), seven who prefer not to say and five selecting other. Residence or work location is Dhaka for 166 records (43.1%); the remaining categories include other cities, district towns and rural areas. These labels describe the records rather than geographic sampling coverage.

Weekly and daily-or-almost-daily AI use together account for 275 records (71.4%). Any formal training is recorded for 160 (41.6%), comprising 106 short orientations and 54 courses or certified training experiences. Fifteen respondents report never using generative AI. That answer is compatible with screening based on having heard of AI and does not warrant exclusion. All 385 observations are complete for the focal analyses, and no missing-value adjustment changes the sample denominator.

4.2 Distributions across distinct privacy judgements

Table 3 reports the complete five-category distributions and endorsement summaries. Keeping the neutral category visible allows the reader to distinguish uncertainty or a middle response from explicit disagreement. Mean differences are described without assuming that the statements measure one common continuum.

Table 3. Privacy item distributions and endorsement

Item	Counts 1 / 2 / 3 / 4 / 5	Mean	SD	Endorsed n (%)	95% CI (%)
PPR1	0 / 29 / 140 / 168 / 48	3.61	0.80	216 (56.1%)	51.1 to 61.0
PPR2	0 / 9 / 85 / 168 / 123	4.05	0.80	291 (75.6%)	71.1 to 79.6
PPR3	0 / 10 / 95 / 190 / 90	3.94	0.76	280 (72.7%)	68.1 to 76.9
PPR4	3 / 23 / 154 / 165 / 40	3.56	0.79	205 (53.2%)	48.3 to 58.2
PPR5	0 / 13 / 68 / 192 / 112	4.05	0.78	304 (79.0%)	74.6 to 82.7

N = 385. Endorsement means agree or strongly agree. Categories 1-5 run from strongly disagree to strongly agree. Wilson

intervals are pointwise; means and SDs are descriptive summaries of ordered responses.

PPR1 disclosure concern is endorsed by 216 respondents (56.1%), with a mean of 3.61 and standard deviation of 0.80. PPR2 self-attributed inhibition is endorsed by 291 (75.6%; mean 4.05, standard deviation 0.80). Conditional willingness under strong privacy controls, PPR3, is endorsed by 280 (72.7%; mean 3.94, standard deviation 0.76). PPR4 meaningful-control preference is endorsed by 205 (53.2%; mean 3.56, standard deviation 0.79). PPR5 attribution to trust has the highest endorsement, 304 (79.0%; mean 4.05, standard deviation 0.78).

Neutral responses are particularly frequent for concern and meaningful control: 140 for PPR1 and 154 for PPR4. These are 36.4% and 40.0% of records respectively. By comparison, 95 respondents select neutral for PPR3 and 68 for PPR5. Strong agreement is recorded for 90 respondents on PPR3 but 40 on PPR4. Thus the ordering between these two safeguard statements remains at the stricter descriptive threshold, although the percentages change substantially.

4.3 Coexistence of concern and conditional willingness

Table 4 reports joint responses. The first panel compares disclosure concern with willingness under strong privacy controls. The second asks whether reported inhibition and conditional willingness are endorsed by the same people. Both panels retain all records, including neutral responses within the non-endorsed category.

Table 4. Joint responses concerning risk and protected use

Item pair	Response combination	Count (%)
PPR1 / PPR3	Both endorsed	162 (42.1%)
	First only	54 (14.0%)
	Second only	118 (30.6%)
	Neither	51 (13.2%)
PPR2 / PPR3	Both endorsed	216 (56.1%)
	First only	75 (19.5%)
	Second only	64 (16.6%)
	Neither	30 (7.8%)

N = 385. PPR1 is concern; PPR2 is attributed inhibition; PPR3 is willingness under strong controls. First and second refer to the listed pair. Non-endorsement includes neutral responses.

Concern and conditional willingness coexist in 162 records (42.1%). Another 54 respondents endorse concern without endorsing PPR3, 118 endorse PPR3 without endorsing concern, and 51 endorse neither. Among the 216 concern-endorsing respondents, 75.0% also endorse conditional willingness. Among the 169 who do not endorse concern, the corresponding proportion is 69.8%. These conditional percentages describe the cross-tabulation and do not estimate a benefit from controls.

Reported inhibition and conditional willingness coexist in 216 records (56.1%). Seventy-five respondents endorse inhibition alone, 64 conditional willingness alone and 30 neither. Of the 291 respondents endorsing inhibition, 74.2% endorse willingness under strong controls. Coexistence is therefore common within this sample, but the joint categories alone do not establish a strong association. They show that endorsement of reluctance for sensitive matters does not preclude endorsement of a more protected

hypothetical service.

4.4 Differences between paired endorsement proportions

Table 5 gives the two selected within-respondent contrasts. The comparisons retain pairing and report the discordant counts from which the exact tests are calculated. Positive differences indicate higher endorsement of the first listed statement.

Table 5. Paired differences in endorsement

Contrast	First only / second only	Difference pp	95% CI pp	Holm p
PPR3 – PPR4	126 / 51	19.5	13.2 to 26.0	<0.001
PPR2 – PPR1	129 / 54	19.5	12.7 to 26.0	<0.001

N = 385; pp = percentage points. Exact McNemar tests are Holm-adjusted within the two-test family. Pointwise percentile intervals use 10,000 paired respondent bootstrap resamples. Wording and conditions differ between items.

PPR3 exceeds PPR4 by 19.5 percentage points, with a pointwise bootstrap interval of 13.2-26.0 points. There are 126 respondents endorsing PPR3 alone and 51 endorsing PPR4 alone. PPR2 exceeds PPR1 by the same rounded difference, 19.5 points, with an interval of 12.7-26.0 points; the discordant counts are 129 and 54. Both comparisons have Holm-adjusted p-values below 0.001. The identical rounded differences result from equal differences in marginal counts, while the uncertainty reflects each paired distribution.

These results establish differences between response proportions under the defined threshold. They do not establish that strong controls are preferred to meaningful control in a direct choice, because the items differ in their referent and wording. Nor does the PPR2-PPR1 contrast show that concern causally produces more inhibition than respondents recognise. Those interpretations would require common conditions and different measurement designs.

4.5 Ordinal relationships with concern

Table 6 retains all ordered response categories. It reports each concern association, its bootstrap interval and its p-value after correction within the four-correlation family. Intervals are pointwise and therefore need not agree with a multiplicity-adjusted threshold decision.

Table 6. Ordinal associations with disclosure concern

Item pair	Spearman ρ	95% CI	Raw p	Holm p
PPR1 / PPR2	-0.028	-0.129 to 0.072	0.582	0.582
PPR1 / PPR3	0.149	0.052 to 0.245	0.003	0.013
PPR1 / PPR4	0.055	-0.041 to 0.151	0.283	0.566
PPR1 / PPR5	0.121	0.022 to 0.222	0.018	0.054

N = 385. Holm correction covers four concern correlations. Bootstrap intervals use 4,000 whole-respondent resamples and are pointwise, not multiplicity-adjusted.

The concern-conditional-willingness association is small and positive: Spearman ρ = 0.149, with a 95% bootstrap interval of 0.052-0.245 and Holm-adjusted p = 0.013. The concern-trust-attribution estimate is 0.121, with an interval of 0.022-0.222, but its adjusted p-value is 0.054. Concern has little estimated ordinal association with reported inhibition (ρ = –0.028; adjusted p = 0.582) or meaningful-control preference (ρ = 0.055; adjusted p = 0.566). Their intervals include both negative and positive values. These findings do not establish

independence or a zero effect in the population.

4.6 Adjusted endorsement models and sensitivity analyses

Table 7 presents both logistic specifications. The model outcomes are endorsement of conditional willingness and endorsement of meaningful-control preference. All five predictors enter each model without automated variable selection. Both models converge on the full sample. Predictor variance inflation factors are close to one, providing no indication of material collinearity in these specifications.

Table 7. Adjusted odds of endorsing the safeguard statements

Outcome	Predictor	aOR	95% CI	Holm p
PPR3	Concern PPR1	1.29	0.98 to 1.69	0.216
	Inhibition PPR2	1.33	1.00 to 1.76	0.190
	Weekly or more AI use	1.02	0.61 to 1.71	—
	Any formal AI training	1.07	0.67 to 1.70	—
	Law student	0.74	0.46 to 1.20	—
PPR4	Concern PPR1	1.17	0.91 to 1.52	0.455
	Inhibition PPR2	1.01	0.78 to 1.30	0.952
	Weekly or more AI use	1.00	0.63 to 1.59	—
	Any formal AI training	1.14	0.75 to 1.72	—
	Law student	0.73	0.48 to 1.11	—

N = 385 in each model. PPR3 outcome: 280 endorsed; PPR4: 205 endorsed. Concern and inhibition are scored per one-point increase. Reference groups are less than weekly AI use, no training and non-student status. Robust sandwich intervals are pointwise. Holm correction covers four focal concern/inhibition tests; covariate intervals are descriptive. aOR is an odds ratio, not a probability ratio.

For PPR3, the adjusted concern odds ratio is 1.29 per one-point increase (95% interval 0.98-1.69; raw p = 0.072; Holm p = 0.216). Reported inhibition has an odds ratio of 1.33 (1.00-1.76; raw p = 0.048), with Holm p = 0.190. For PPR4, the concern estimate is 1.17 (0.91-1.52; Holm p = 0.455), while inhibition is 1.01 (0.78-1.30; Holm p = 0.952). None of the four focal model tests meets the 0.05 threshold after adjustment. Odds ratios concern the response threshold and are not percentage increases in adoption probability.

Table 8 reports additional sensitivity analyses. Student restriction and alternative concern coding assess interpretation under changed analytical choices; they do not provide independent replication.

Table 8. Subset sensitivity for the adjusted concern association

Item	Subset	n	Endorsed n (%)	aOR	95% CI
PPR3	Law students	242	171 (70.7%)	1.23	0.88 to 1.72
PPR3	Other respondents	143	109 (76.2%)	1.41	0.84 to 2.34
PPR4	Law students	242	122 (50.4%)	1.23	0.90 to 1.69
PPR4	Other respondents	143	83 (58.0%)	1.09	0.70 to 1.69

Separate models adjust for reported inhibition, weekly-or-more AI use and any training. Law-student status is constant within each subset and is omitted. Intervals are robust and pointwise. These subset estimates do not test an interaction and are not independent replications of the full-sample analysis.

Among 242 law students, 171 (70.7%) endorse PPR3 and 122 (50.4%) endorse

PPR4. Among 143 other respondents, the counts are 109 (76.2%) and 83 (58.0%). Adjusted concern estimates remain positive in each subset, with intervals spanning one. Replacing linear concern scoring with category indicators gives joint robust Wald p-values of 0.193 for PPR3 and 0.599 for PPR4. This does not establish linearity, but it provides no strong evidence of a concern association concealed by the selected scoring. The ordinal and binary results together indicate a modest rank relationship whose evidence is weaker at the agreement threshold after limited adjustment.

5. Discussion

The principal finding is that privacy-related restraint and interest in protected AI legal services frequently coexist. Their coexistence is descriptively clear, while adjusted associations at the endorsement threshold remain uncertain. The discussion interprets that distinction through privacy calculus and measurement specificity, then considers what it implies for the design and evaluation of legal platforms.

5.1 Privacy restraint and conditional acceptance

More than half of the sample simultaneously endorses privacy-related inhibition and greater willingness under strong controls. These statements describe different conditions. A person may avoid using an inadequately protected service for a sensitive matter while remaining interested in a service that addresses that concern. This interpretation is compatible with the balance of inhibiting and encouraging considerations in privacy calculus.[30] It does not require respondents to regard exposure as harmless or to accept a platform unconditionally.

The joint count is more informative than a comparison of overall percentages because it identifies coexistence within the same records. However, common endorsement should not be mistaken for a large statistical relationship. PPR2 and PPR3 are both often endorsed, so a sizeable overlap can occur even with a modest association. The adjusted inhibition estimate for PPR3 is positive but does not meet the corrected threshold. The defensible conclusion is that the recorded inhibition judgement is compatible with conditional willingness; the study does not establish inhibition as a reliable determinant of that willingness.

This distinction changes the practical question. A provider cannot conclude that concern is simply an obstacle to remove through reassurance. It needs to determine what protection the contemplated task requires, whether users understand its limits

[30] Dinev and Hart (n 5).

and whether a suitable service remains useful under those constraints. A future experiment could compare a general assurance with a concrete retention or access control while keeping the legal task fixed. That design would identify a response to a specified safeguard more directly than an agreement item.

5.2 Why the ordinal and binary results differ

Concern has a small positive rank association with PPR3, while the corresponding adjusted endorsement estimate is less precise. The analyses answer different questions. Spearman correlation uses all ordered categories; the logistic model distinguishes agreement or strong agreement from the remaining responses and conditions on four other predictors. Information that separates strong agreement from agreement can contribute to the ordinal relationship without moving a respondent across the binary threshold.

Consequently, the adjusted result should not be described as contradicting or disproving the ordinal finding. Neither should the corrected correlation be promoted as evidence that concern causes adoption. Both analyses concern answers collected together, and a common response tendency or unmeasured experience could contribute to their relationship. Statistical interpretation should consider the effect size, the uncertainty and the question being estimated, rather than whether a single p-value crosses a conventional boundary.[31]

The magnitude of $\rho = 0.149$ is also relevant. It indicates limited rank alignment, not a broad explanatory account of conditional willingness. A concern statement cannot explain service choice without measures of the task, expected benefit and available alternatives. The weaker threshold result therefore helps delimit the finding. It suggests that a general association among levels of agreement should be investigated through more specific decisions before it informs an adoption model.

5.3 Strong protection and meaningful user control

Endorsement of strong privacy controls exceeds endorsement of meaningful data control by 19.5 percentage points. This difference is large enough to merit further investigation, but its meaning remains open. PPR3 asks about being more willing under a protective condition, whereas PPR4 asks about preferring a platform that gives meaningful control. The wording differs in comparative structure, emphasis and reference to legal platforms. It therefore cannot isolate the value respondents assign to technical protection relative to personal agency.

The control-paradox experiments provide a reason to assess how control affects disclosure as well as perceived safety.[32] They do not imply that this sample exhibits

[31] Ronald L Wasserstein and Nicole A Lazar, 'The ASA Statement on p-Values: Context, Process, and Purpose' (2016) 70 American Statistician 129.

[32] Brandimarte, Acquisti and Loewenstein (n 14).

that paradox. Here, no information was disclosed to an AI legal service as an observed study outcome, and no control was manipulated. Similarly, privacy-assurance research motivates examining the credibility of safeguards rather than assuming that users interpret every assurance identically.[33]

A useful next step is to define control through concrete operations. For example, a participant could decide whether a document is retained after a task or identify which recipients can access it. Investigators should verify that the interface enforces those choices and measure whether users understand the consequences. A control that is technically effective but misunderstood and a reassuring interface that fails to restrict processing pose different problems. The present findings identify interest in this distinction without resolving it.

5.4 Concern is not a complete account of inhibition

The estimated concern-inhibition correlation is close to zero even though inhibition is more frequently endorsed. That result does not show that privacy concern has no relevance to use. PPR1 asks about worry over exposure, while PPR2 asks whether privacy concerns reduce willingness for sensitive matters. The latter includes a judgement about one's motivation and a more specific task context. Their meanings do not guarantee that respondents will order themselves similarly on both statements.

Context-sensitive work on disclosure reinforces the need to specify the circumstances rather than treat every privacy judgement as interchangeable.[34] The current instrument does not record an experienced breach, the urgency of the legal problem, availability of a human adviser or the respondent's understanding of data processing. Those are possible explanations to investigate, not measured reasons for the current result. Privacy fatigue is likewise a candidate for future study only when exhaustion or disengagement is assessed directly.[35]

The appropriate response is better measurement rather than selective item removal. Low alpha is consistent with the block's heterogeneous content, but statistical consistency alone could not establish a valid adoption construct.[36] Risk, behavioural inhibition and protective preferences should be independently specified in subsequent research. That would allow researchers to test whether concern predicts a defined action, instead of relying on an item that already states the proposed influence.

[33] Bansal, Zahedi and Gefen, ‘Privacy Assurance’ (n 15).
[34] Bansal, Zahedi and Gefen, ‘Context and Personality’ (n 15).
[35] Choi, Park and Jung (n 21).
[36] Sijtsma (n 25).

5.5 Legal confidentiality and the limits of user choice

Legal-service privacy extends beyond the immediate user's preference. A case narrative may identify other people, and the person seeking assistance may not control every relevant interest. Contextual integrity helps explain why appropriate information flows depend on roles and transmission conditions.[37] The survey does not identify actual client matters or breaches, so it cannot establish that any participant has mishandled information.

Comparative ABA guidance places confidentiality within the responsibilities of lawyers using generative AI.[38] That guidance is discussed as a comparative professional source rather than binding Bangladesh law. The domestic constitutional and statutory context is separately identified in Section 1.1. Because fieldwork timing is unknown, the study also avoids attributing any response pattern to the 2026 legislation. The findings support questions about usable safeguards, while legal duties must be determined from applicable law and the particular service.

An implication is that consent should not be treated as a substitute for all organisational protection. Even where a user wishes to proceed, a provider should evaluate the actual data flow, necessary information and possible consequences. NIST's privacy framework offers a systematic risk-management reference for that evaluation.[39] This is a normative design recommendation informed by the survey's subject, rather than an observed preference for every component of the framework.

5.6 Integrated theoretical interpretation

The survey contributes a differentiated description of potential acceptance. Concern can accompany willingness under a stated protective condition; attributed inhibition is common; and a trust-attribution statement receives high endorsement without measuring trust itself. These results preserve distinctions needed by privacy-calculus, protection-motivation and planned-behaviour accounts. They do not validate a full integrated theory.

Protection motivation would require independent coping-efficacy measures to explain how a control changes action.[40] Planned behaviour would require a specified prospective action and the relevant social and control constructs.[41] The present analysis instead identifies what a future model must keep separate. Its contribution is empirical clarification of a legal-platform decision, with associations that are modest or uncertain and a clear distinction between potential protected use and actual adoption.

[37] Nissenbaum (n 16).
[38] American Bar Association (n 1).
[39] NIST (n 8).
[40] Maddux and Rogers (n 11).
[41] Ajzen (n 13).

6. Theoretical and Practical Implications

The implications follow from the separation of measured judgements. Some concern research design; others propose features and evaluation procedures for providers and educators. The survey did not test the effectiveness of an intervention, and the recommendations therefore specify what should be evaluated rather than promise an adoption increase.

6.1 Implications for theory and measurement

The first theoretical implication is that acceptance should include its conditions. A person who expresses reluctance for sensitive matters but interest in a protected platform is not necessarily located at two contradictory points on a single acceptance scale. The conditions differ. A future privacy-calculus model should therefore distinguish unconditional willingness, willingness under stated protections and observed decisions. Independent benefit and trust measures would then permit a more complete assessment of the proposed trade-off.

Second, the object of concern needs to match the action. Worry about exposure from a general legal platform can be studied separately from willingness to disclose a particular document. The concern-inhibition finding demonstrates the analytical cost of assuming equivalence between an emotion and an attributed behavioural influence. A matched design could vary information sensitivity while holding the task and platform constant. It could then test whether concern explains choices under otherwise comparable conditions.

Third, threshold choice belongs in theoretical interpretation. A rank relationship and an adjusted endorsement comparison need not provide the same evidence. Researchers should define the decision of substantive interest before selecting a scale or cut-off. Reporting both full distributions and a justified threshold makes the relationship between theory and analysis visible. Recent privacy syntheses support this attention to differentiated contexts and relationships, without supplying a universal coefficient that should be expected in every setting.[42]

6.2 Implications for platform design and legal education

Providers can translate a broad promise of protection into verifiable task conditions. Before a user submits a legal document, an interface could explain the intended processing, relevant recipients and retention arrangement in language the user understands. Information that is unnecessary for the task should be omitted where feasible. The provider should verify that the technical configuration matches the explanation and record how exceptions are handled. These are proposed evaluation criteria, not features measured in the survey.

User control should also be tested for comprehension. A study could ask participants to restrict access or choose a retention setting, then assess whether they understand the resulting information flow.

[42] Herriger and others (n 7); Luu and Harrison (n 7).

Evaluation should record both successful task completion and unnecessary disclosure. The current PPR3-PPR4 difference identifies a reason to examine these outcomes separately. It does not establish that people prefer simplified assurances or that a particular control interface will increase use.

Legal education can use fictional case files to teach these decisions without exposing real clients. Students could identify which details are essential, which identify third parties and whether a public AI service is suitable for the task. The exercise should include situations in which withholding information or consulting a supervisor is the appropriate action. Competence would be demonstrated through the choice and its justification, rather than an agreement score. Technical evidence on extraction and inference provides background for explaining why removing an obvious name may not resolve every privacy issue.[43]

6.3 Implications for governance and evaluation

The high endorsement of trust's influence suggests that protection is salient to respondents' stated intentions, but it does not demonstrate trustworthy processing. Governance should evaluate service arrangements independently of favourable answers. A provider can combine documented responsibilities, testing of privacy risks and usable routes for questions or correction. The NIST generative-AI profile supplies a broader reference for organising this work.[44]

For Bangladesh, evaluation should distinguish current legal requirements from hypothetical preferences and should document the law in force at the relevant time. A later survey could ask about specific rights only after the applicable provisions and terminology have been checked. This study makes no estimate of legal compliance or public knowledge of the 2026 Act. Its contribution is a set of empirically grounded questions about the conditions under which respondents contemplate using AI legal services.

7. Conclusion Limitations and Future Research

In the 385 analysed records, privacy-related restraint frequently coexists with willingness to use a platform under stronger protections. Conditional willingness is endorsed by 72.7%, reported inhibition by 75.6%, and both by 56.1%. Concern has a small positive ordinal association with conditional willingness, but adjusted endorsement models provide uncertain estimates after correction. Strong privacy controls and meaningful control over personal data also attract different levels of agreement. These are distinct questionnaire responses, not observed effects on platform adoption.

The article contributes a way to examine privacy and potential acceptance without collapsing concern, inhibition, conditional willingness and trust attribution into one score. It shows why a positive response to a safeguard condition cannot be read as unconditional acceptance or permission for

[43] Carlini and others (n 2); Staab and others (n 2).
[44] Autio and others (n 18).

unrestricted disclosure. It also shows why common endorsement within a sample should be separated from the strength of an estimated association. These distinctions provide a basis for more precise legal-technology research.

The study's limits concern design, measurement and provenance. Cross-sectional self-reports do not establish temporal order or causality. There is no named-platform task, observed disclosure or unconditional adoption outcome. The sample combines students, graduates, professionals and other respondents; recruitment, dates and response rates are undocumented. Source records are needed to explain the Codebook's synthetic identifier and contextual-comment labels, although the numerical responses are supplied as real data. The comments were excluded. Conventional intervals and covariate adjustment cannot resolve selection bias or independently authenticate the records.

Future research should first establish a documented sampling process and preserve the wording, consent and data-processing records. Cognitive interviews can test how participants interpret “strong privacy controls” and “meaningful control”. A revised instrument should independently measure concern, perceived benefit, trust, efficacy and a specific prospective intention. Longitudinal observation could then connect those measures with later choices rather than asking respondents to attribute influences within a single statement.

A complementary experiment could use fictional legal tasks, vary a concrete safeguard and observe what information participants choose to submit. The design should hold utility and task sensitivity constant where possible, verify that the control works and assess comprehension. Outcomes should include justified non-use, unnecessary disclosure and successful completion. Such evidence would allow researchers to ask whether protections enable appropriately informed engagement. The present findings identify that question and its measurement requirements; they do not pre-empt the answer.

Declarations

Ethical approval and oversight

Formal ethical approval was not obtained because the authors' institutional setting did not provide an accessible review mechanism applicable to this non-interventional adult questionnaire study. Informed consent, voluntary participation, anonymity, discontinuation and aggregate reporting were followed, as detailed in Section 3.7.

Informed consent

Consent preceded questionnaire completion. All analysed records contain affirmative consent and adult-eligibility responses.

Data availability

De-identified numerical data and analytical specifications may be requested from the corresponding author, subject to confidentiality and applicable institutional requirements. Contextual comments were excluded.

Funding and competing interests

The authors report no external funding and no competing interests.

Author contributions

Farhan Islam: Conceptualisation; preparation of study materials; data preparation and curation; manuscript development. Prof. Dr Kazi Abdul Mannan: Methodological guidance; supervision; interpretation of findings; critical review and editing.

Generative AI disclosure

Generative AI assisted literature searching, drafting, language editing, organisation and analytical-code development. Estimates were calculated programmatically from the supplied numerical records. The authors are responsible for the analysis, interpretation, source verification and final manuscript, including compliance with the target journal's disclosure policy.

Personal Data Protection Act 2026 (Bangladesh) (Act No 63 of 2026), ss 1 and 44 <https://bdlaws.minlaw.gov.bd/act-details-1692.html> accessed 28 October 2026

Bibliography

Ajzen I, ‘The Theory of Planned Behavior’ (1991) 50 Organizational Behavior and Human Decision Processes 179

American Bar Association Standing Committee on Ethics and Professional Responsibility, ‘Generative Artificial Intelligence Tools’ (Formal Opinion 512, 29 July 2024)

Autio C and others, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1, National Institute of Standards and Technology 2024)

Bansal G, Zahedi FM and Gefen D, ‘Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online’ (2016) 53 Information & Management 1

Bansal G, Zahedi FM and Gefen D, ‘The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern’ (2015) 24 European Journal of Information Systems 624

Baruh L, Seçinti E and Cemalc■lar Z, ‘Online Privacy Concerns and Privacy Management: A Meta-Analytical Review’ (2017) 67 Journal of Communication 26

Brandimarte L, Acquisti A and Loewenstein G, ‘Misplaced Confidences: Privacy and the Control Paradox’ (2013) 4 Social Psychological and Personality Science 340

Carlini N and others, ‘Extracting Training Data from Large Language Models’ in *30th USENIX Security Symposium* (USENIX Association 2021) 2633

Choi H, Park J and Jung Y, ‘The Role of Privacy Fatigue in Online Privacy Behavior’ (2018) 81 Computers in Human Behavior 42

Cochran WG, *Sampling Techniques* (3rd edn, John Wiley & Sons 1977)

Dinev T and Hart P, ‘An Extended Privacy Calculus Model for E-Commerce Transactions’ (2006) 17 Information Systems Research 61

Efron B and Tibshirani RJ, *An Introduction to the Bootstrap* (Chapman & Hall 1993)

Herriger C and others, ‘Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, Augmented Reality, Big Data, and the

Internet of Things: Systematic Review' (2025) 27 Journal of Medical Internet Research e71951

Holm S, 'A Simple Sequentially Rejective Multiple Test Procedure' (1979) 6 Scandinavian Journal of Statistics 65

Hosmer DW Jr, Lemeshow S and Sturdivant RX, *Applied Logistic Regression* (3rd edn, John Wiley & Sons 2013)

Johnston AC and Warkentin M, 'Fear Appeals and Information Security Behaviors: An Empirical Study' (2010) 34 MIS Quarterly 549

Luu T and Harrison A, 'Understanding Information Privacy Concerns: A Meta-Analytic of Three Decades of Research' (2026) Information Systems Research, advance online publication, doi:10.1287/isre.2023.0797

Maddux JE and Rogers RW, 'Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change' (1983) 19 Journal of Experimental Social Psychology 469

Malhotra NK, Kim SS and Agarwal J, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model' (2004) 15 Information Systems Research 336

McNemar Q, 'Note on the Sampling Error of the Difference between Correlated Proportions or Percentages' (1947) 12 Psychometrika 153

National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (version 1.0, 2020)

Nissenbaum H, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119

Sijtsma K, 'On the Use, the Misuse, and the Very Limited Usefulness of Cronbach's Alpha' (2009) 74 Psychometrika 107

Smith HJ, Dinev T and Xu H, 'Information Privacy Research: An Interdisciplinary Review' (2011) 35 MIS Quarterly 989

Solove DJ, 'The Myth of the Privacy Paradox' (2021) 89 George Washington Law Review 1

Staab R and others, 'Beyond Memorization: Violating Privacy via Inference with Large Language Models' in *The Twelfth International Conference on Learning Representations* (2024) <https://proceedings.iclr.cc/paper_files/paper/2024/hash/9028b8a3ca98f58e373f0c1497a17448-Abstract-Conference.html> accessed 28 October 2026

von Elm E and others, 'The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies' (2007) 4 PLOS Medicine e296

Wasserstein RL and Lazar NA, 'The ASA Statement on p-Values: Context, Process, and Purpose' (2016) 70 American Statistician 129

White H, 'A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity' (1980) 48 Econometrica 817

Wilson EB, 'Probable Inference, the Law of Succession, and Statistical Inference' (1927) 22 Journal of the American Statistical

Association 209

Appendix A Questionnaire wording

Table A1 provides the exact focal wording so that the statistical results can be read against the conditions stated in each question.

Table A1. Exact wording of the focal statements

Code	Questionnaire statement
PPR1	I worry that AI-powered legal platforms may expose personal or confidential information.
PPR2	Privacy concerns reduce my willingness to use AI services for sensitive legal matters.
PPR3	I would be more willing to use an AI platform that offers strong privacy controls.
PPR4	I would prefer an AI legal platform that allows meaningful control over personal data.
PPR5	Trust in data protection affects my intention to adopt AI-powered legal services.

Source: supplied Group 5 questionnaire and workbook Codebook. Responses: 1 strongly disagree, 2 disagree, 3 neutral, 4 agree, 5 strongly agree.

PPR2 and PPR5 attribute influences within their wording. PPR3 and PPR4 refer to protective conditions and control preferences. No statement records an actual adoption event.

Table of legislation

The Constitution of the People’s Republic of Bangladesh, art 43