Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

AI Awareness and Personal Data Protection Practices in Bangladesh

Dr Kazi Abdul Mannan

drkaziabdulmannan@gmail.com

Center for Academic & Professional Career Development and Research (CAPCDR)
https://orcid.org/0000-0002-7123-132X

Moumita Akter Mira

Shanto-Mariam University of Creative Technology https://orcid.org/0009-0009-8989-7566

Research Article

Keywords: AI awareness, personal data protection, privacy literacy, sensitive information, generative AI, Bangladesh, self-reported behaviour

Posted Date: November 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11602441/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

AI Awareness and Personal Data Protection Practices in Bangladesh

Moumita Akter Mira

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

Email: mou383533@gmail.com

ORCID: https://orcid.org/0009-0009-8989-7566

Prof. Dr Kazi Abdul Mannan

Department of Business Administration, Faculty of Business, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh

Email: drkaziabdulmannan@gmail.com

ORCID: https://orcid.org/0000-0002-7123-132X

Abstract

Generative artificial intelligence creates opportunities for learning and professional work while requiring users to make decisions about sensitive information. This study examines whether self-reported AI awareness aligns with two distinct personal-data protection practices in Bangladesh: avoiding sensitive information in public AI tools and checking privacy or data-use information before sensitive tasks. A cross-sectional analysis of 385 adult respondents uses item-level distributions, paired endorsement contrasts, proportional-odds models and direct comparison of outcome-specific coefficients. The sample includes 242 law students alongside graduates, legal professionals and other respondents; it is not representative of all university students or the national population. Checking privacy information was endorsed by 284 respondents (73.8%), compared with 222 (57.7%) for avoiding sensitive input. Their within-person difference was 16.1 percentage points (95% bootstrap interval 9.6–22.6; Holm-adjusted $p < .001$). Self-reported understanding of privacy risks was endorsed by 275 respondents (71.4%), whereas understanding that AI services may collect, store or process user data was endorsed by 177 (46.0%). None of the eight focal awareness–practice coefficients received clear support after Holm correction; the joint comparison of associations across the two practices was inconclusive ($\chi^2(4) = 1.83$, $p = .768$). The findings distinguish self-reported understanding, reported protective practices and their uncertain adjusted relationships. Privacy calculus and protection motivation theory inform interpretation, but the questionnaire does not measure all components required to test either theory. Future research should document recruitment and evaluate privacy decisions through observed tasks or experiments involving specific AI services.

Keywords: AI awareness; personal data protection; privacy literacy; sensitive information; generative AI; Bangladesh; self-reported behaviour

1 Introduction

People use generative artificial intelligence to draft text, find ideas, interpret information and support learning. These activities may involve entering descriptions, documents or questions into an external service. The privacy implications depend on the information disclosed, the service's processing practices and the context in which the tool is used. UNESCO's guidance on generative AI in education and research places data protection alongside human agency and institutional responsibility. The present study examines respondents' stated awareness and protective practices in this setting, without assuming that every AI service handles information in the same way.[1]

A decision to avoid sensitive input differs from a decision to consult information about how data are used. The first concerns what a person says they withhold from public AI tools; the second concerns what they say they check before sensitive tasks. A person could perform one, both or neither. Understanding a general privacy risk also differs from knowing that services may collect, store or process data. These distinctions are the basis of the study's analysis. Treating all such statements as a single awareness or behaviour score would obscure differences in content and make the results less useful for education and governance.

The study draws on the Group 5 Law–SDG survey in Bangladesh. Its numerical records contain responses to separate items about privacy-risk understanding, processing awareness, avoiding sensitive input and checking privacy information. These are self-reports, not observations of completed tasks or independent tests of knowledge. The data do not establish what respondents actually entered into an AI system, whether they read a particular notice or whether a specific provider retained information. The purpose is to study how respondents describe these practices and expectations within the supplied sample.

Bangladesh's Personal Data Protection Act 2026 provides an important legal context for personal-data processing. The Act addresses access and correction, transparent processing and security in relevant provisions. Its section 1(3) provides for most provisions to be deemed effective from 6 November 2025, while section 23 and sections 31–35 have a separate later commencement mechanism involving notification after the period specified in the Act. Application to an individual service or data-processing activity depends on scope, statutory conditions, exceptions and implementation. The survey does not establish legal compliance or a violation.[2]

Universities face a practical distinction between educating users and governing the systems made available to them. Training may help a student recognise a risk, but an individual's ability to understand and control a service also depends on the clarity of its information, available settings and institutional arrangements. The survey contains no direct assessment of an institution's policies or a service's interface. Its contribution is to identify questions that a

[1] Fengchun Miao and Wayne Holmes, *Guidance for Generative AI in Education and Research* (UNESCO 2023) <https://doi.org/10.54675/EWZM9535> accessed 27 October 2026.

[2] Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 1; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 11; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 12; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 15.

future intervention should address: what do users say they understand, which protective steps do they report and how do these responses differ?[3]

Privacy research has long considered why stated concerns, knowledge and behaviour do not always move together. A meta-analysis by Baruh, Secinti and Cemalcilar identified relationships between online privacy concerns, literacy and protective measures, while Barth and de Jong reviewed discrepancies between expressed concerns and behaviour. These studies provide a broader empirical context, but neither establishes a causal pathway in the present Bangladesh sample. A gap between agreement with two questionnaire statements should not automatically be called a privacy paradox: the statements have different wording, and both are self-reported.[4]

The central research problem is whether respondents who report greater AI awareness also report stronger protection practices, and whether different practices show the same pattern. The survey measures four awareness-related propositions separately: understanding privacy risk from information entered into AI, understanding possible data processing, recognising plausible inaccuracy, and awareness of biased or incomplete outputs. Two outcome items record reported avoidance of sensitive input and checking of privacy information. General verification practice and three contextual characteristics are included as covariates. This design makes each item's meaning visible and avoids claiming an unmeasured latent awareness effect.

The article makes three contributions. First, it compares two self-reported practices within the same respondents rather than treating one as a proxy for the other. Second, it examines whether two kinds of privacy-related understanding are endorsed at different rates. Third, it compares the adjusted associations for the two practices using the correlation of responses from the same people. A joint comparison provides a more appropriate test of differing association patterns than observing that one coefficient appears significant and another does not.

The objectives are to report the complete distributions of relevant questionnaire items; examine paired differences between checking and avoidance and between the two privacy-understanding items; estimate exploratory associations of awareness with each reported practice; and directly compare those associations across outcomes. The analyses cover all 385 eligible records, with sensitivity analyses for sample composition and AI-use history.

The research questions are: how often are each of the two practices reported; do their endorsement rates differ within respondents; how frequently are risk and processing understanding endorsed; and are the four awareness items associated with either practice after adjustment? A further question asks whether the four association patterns differ between practices. These are observational questions. They do not ask whether teaching awareness causes a change in behaviour, and the survey cannot answer that causal question.

[3] Lemi Baruh, Ekin Secinti and Zeynep Cemalcilar, 'Online Privacy Concerns and Privacy Management: A Meta-Analytical Review' (2017) 67 Journal of Communication 26; Miao and Holmes (n 1).

[4] Baruh, Secinti and Cemalcilar (n 3); Susanne Barth and Menno DT de Jong, 'The Privacy Paradox: Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review' (2017) 34 Telematics and Informatics 1038.

Section 2 develops the theoretical and legal foundation; Section 3 explains the data and analysis; Section 4 reports the results; and Sections 5–7 interpret their significance, implications and limitations.

2 Literature Review and Theoretical Foundation

This review connects privacy awareness and protective practices with theories of privacy-related decision-making. It distinguishes a general account of risk–benefit evaluation from a theory of coping with threats and from a theory of planned behaviour. These frameworks generate useful questions, but each requires constructs that are not all present in the supplied questionnaire. Their role in this article is therefore to guide interpretation and a future research agenda rather than to claim confirmation of an unmeasured structural pathway.

2.1 Privacy literacy and AI-related practices

Privacy literacy can include knowledge of data practices, risks, rights and protective options. Baruh and colleagues' synthesis found relationships between privacy literacy and protective measures across a broad online literature. Recent work in the Middle East and North Africa has also examined privacy literacy and protection using mixed methods, while a 2026 meta-analysis connects perceived control and privacy concerns with several online privacy behaviours. These studies motivate attention to understanding and action but should not be transferred mechanically to a different instrument or population.[5] The current items ask respondents what they believe they understand or do; they do not test their answers against a correct service-specific description.[6]

DPA1 asks whether respondents understand that information entered into an AI system may create privacy risks. DPA4 asks whether they understand that AI services may collect, store or process user data. These statements overlap but are not identical. Someone can recognise a general possibility of risk without knowing the details of a service's data lifecycle. Conversely, understanding that processing occurs does not establish that a person knows whether a particular processing activity is unlawful or harmful. Both items are treated as self-assessments rather than verified knowledge.

DPA2 records avoiding sensitive personal information in public AI tools. DPA3 records checking privacy or data-use information before using an AI service for sensitive tasks. These practices differ in timing, object and specificity. Avoidance concerns input; checking concerns information about a service. DPA3 does not establish whether the information consulted is complete, understood or applied. DPA2 does not establish that the respondent never discloses sensitive information in another environment. The distinction matters because a recommendation to improve one practice cannot be assumed to improve the other.

[5] Walaa Bajnaid and Shuaa Aljasir, 'Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region' (2025) 6 Journalism and Media 8; Jana Dombrowski and Sabine Trepte, 'Taking Stock of Social Media Privacy: Meta-Analytic Evidence on How Control, Trust, and Concerns Are Associated with Social Media Use, Disclosure, and Protection' (2026) 31 Journal of Computer-Mediated Communication zmaf025.

[6] Baruh, Secinti and Cemalcilar (n 3).

2.2 Privacy calculus

Privacy calculus scholarship considers how people evaluate benefits, risks and other considerations when deciding whether to disclose information. Dinev and Hart's model includes privacy concerns, trust and perceived benefits in an e-commerce setting. Its value for the present article lies in highlighting that a disclosure choice may involve more than awareness of risk. Educational usefulness, convenience, trust in a provider and the availability of alternatives can all be relevant questions. Their presence and effects are not directly measured in the Group 5 analysis.[7]

The questionnaire lacks a full set of perceived benefits, trust, risk magnitude and disclosure-choice measures needed to estimate a privacy-calculus mechanism. Wording such as "AI awareness causes protective behaviour through privacy calculus" would therefore exceed the evidence. Instead, the two practice items can serve as starting points for a later study that asks respondents to evaluate concrete service terms, the value of a task and the information they would disclose. The relevant comparison is not whether an abstract theory sounds plausible but whether its components are measured separately and under defined conditions.

This distinction is especially relevant to AI services because a task may appear simple while its data implications are difficult to assess. A user may be able to see a privacy statement but not know whether it applies to a particular account or institutional contract. Another user may avoid identifiable details while overlooking information that can be combined with other data. These are possible design and educational challenges, not empirical findings of the present survey. They point to the need for service-specific tests of comprehension and decisions.

2.3 Protection motivation and planned behaviour

Protection motivation theory distinguishes threat appraisal from coping appraisal. A person may recognise a threat while doubting whether a proposed response is effective, affordable or within their control. This perspective helps explain why awareness alone may be insufficient to predict a protective act. It also provides a reason to measure perceived response efficacy and confidence alongside risk recognition. The questionnaire used here does not contain a complete set of these measures, so the present models do not test a protection-motivation mediation or moderation pathway.[8]

The theory of planned behaviour addresses relationships among attitudes, perceived social expectations, perceived control and intention. It is useful for identifying further determinants of behaviour, but its constructs cannot be inferred simply from item labels. DPA2 and DPA3 are framed as reported practices rather than a full validated behavioural intention scale. The models do not estimate perceived behavioural control, subjective norms or intentions as a

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

[8] Ronald W Rogers, 'A Protection Motivation Theory of Fear Appeals and Attitude Change' (1975) 91 Journal of Psychology 93.

sequence. TPB remains a supporting conceptual reference rather than a tested structural model.[9]

Integrating these perspectives suggests a testable future proposition: privacy knowledge may be connected with protective behaviour only when users can recognise a relevant choice, perceive a response as effective and have access to a workable alternative. This is a research proposition, not a conclusion from the present estimates. Its evaluation would require prospective or experimental data, distinct measures and attention to institutional as well as individual resources.

2.4 Self-report and the privacy paradox

The privacy-paradox literature examines differences between expressed privacy attitudes and subsequent conduct. Barth and de Jong caution that the relationship is context-dependent. The current study compares agreement with different statements at one time and does not observe actual disclosures. Even a significant difference between risk understanding and reported avoidance does not demonstrate that people knowingly act against their preferences. The items can differ in interpretation, task reference and response difficulty.[10]

Self-report can still provide useful information about the practices respondents believe they use. Its value increases when item wording, response distributions and limitations are reported clearly. The two-item practice comparison in this study is therefore accompanied by a joint table showing the same respondents' endorsements, including neutrality within non-endorsement. It is not presented as a behavioural ranking under equal experimental conditions.

Common-source measures can also share response tendencies. An association between an awareness statement and a practice statement could reflect real alignment, a general tendency to agree, or factors not included in the model. Podsakoff and colleagues' discussion of common-method bias supports acknowledging this issue without assuming that a single statistical test can quantify or remove it. Future work can combine survey responses with observed tasks and service-specific knowledge checks.[11]

2.5 Legal and institutional safeguards

The Personal Data Protection Act 2026 provides a general framework for handling personal data within its scope. Section 11 addresses access to processed data; section 12 concerns correction and updating; section 15 concerns transparency and accountability; and section 17 addresses security measures. The wording of these provisions and any applicable regulations matter in a particular case. A respondent's belief that a service processes data does not establish whether the service has complied with these duties.[12]

---

[9] Icek Ajzen, 'The Theory of Planned Behavior' (1991) 50 Organizational Behavior and Human Decision Processes 179.

[10] Barth and de Jong (n 4).

[11] Philip M Podsakoff and others, 'Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies' (2003) 88 Journal of Applied Psychology 879.

[12] Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 11; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 12; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 15; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 17.

The Act is not merely proposed legislation. Under section 1(3), most provisions are deemed effective from 6 November 2025, while the provisions specified for later commencement follow a separate notification mechanism. The legal context is presented with this distinction so that recommendations for education are not confused with claims about when every provision took effect. The research does not assess enforcement, legal awareness or a specific provider's practices.[13]

Institutional safeguards also determine what individual action is possible. A clear notice, a choice of account settings, guidance on sensitive material and an accessible route for questions can support users' decisions. However, a notice does not guarantee comprehension, and access to settings does not establish that a system is safe for every category of information. The distinction between individual practices and organisational design follows broader work on accountable data processing.[14]

2.6 Exploratory propositions and framework

Four focal awareness items are examined in relation to each reported practice. H1 concerns self-reported understanding that AI input may create privacy risks (DPA1). H2 concerns understanding that AI services may collect, store or process data (DPA4). H3 concerns awareness that generative AI can produce plausible inaccuracies (AIL1). H4 concerns awareness that outputs may reflect bias or incomplete data (AIL3). These items are entered separately because their contents are not interchangeable. Their hypothesised positive associations are exploratory and apply separately to DPA2 and DPA3, producing eight focal coefficients.

The two privacy-specific items have a direct conceptual connection to data protection, whereas inaccuracy and bias awareness reflect broader AI literacy. A respondent who recognises that an output can be incorrect may not necessarily know a provider's data practices. Equally, awareness of data processing may coexist with uncertainty about what to do. The model examines response alignment without assuming that these understandings form a validated scale or cause a practice.[15]

Figure 1 displays the exploratory framework. The arrows represent statistical associations with two separate self-reported outcomes, with general verification, training, AI-use frequency and age included as contextual covariates. No mediation, experimentally induced awareness or observed disclosure is represented. Direct comparison of corresponding slopes accounts for the fact that both outcomes were measured in the same records.

[13] Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 1.

[14] Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13 European Law Journal 447; Miao and Holmes (n 1).

[15] Davy Tsz Kit Ng and others, 'Conceptualizing AI Literacy: An Exploratory Review' (2021) 2 Computers and Education: Artificial Intelligence 100041; Baruh, Secinti and Cemalcilar (n 3).

Figure 1. Exploratory awareness–practice framework. Arrows represent associations rather than causal effects.

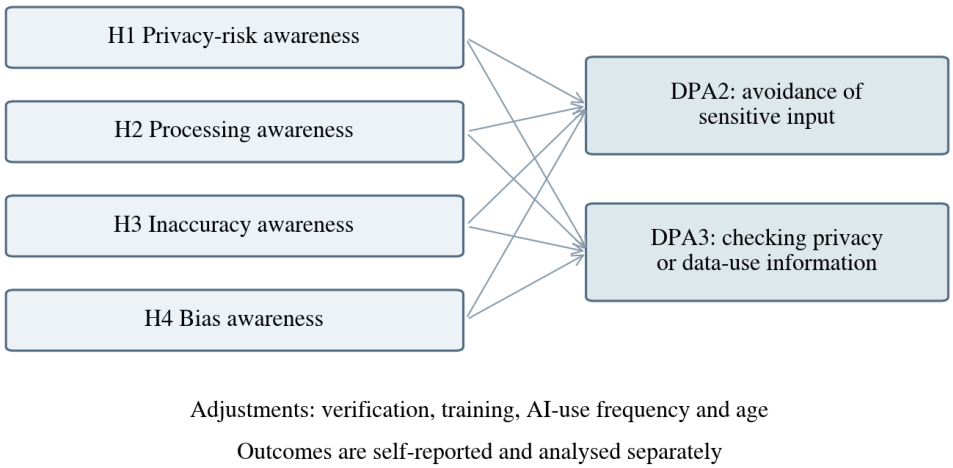


Figure 1. Exploratory awareness–practice framework.

The framework permits descriptive and adjusted findings to differ. A practice can be endorsed frequently even when the measured awareness items do not explain much variation in its responses. The following methodology makes this distinction explicit through paired comparisons, ordinal modelling and uncertainty reporting.

3. Methodology

The study uses a cross-sectional quantitative analysis of the numerical Group 5 survey records and the accompanying Codebook. The design is descriptive and exploratory. It retains separate item meanings, reports all 385 eligible records, and compares the two outcome responses within persons. The study does not estimate causal effects of AI education or present the questionnaire as a validated structural model of privacy behaviour.

3.1 Data source and sample

The research team confirmed that the numerical responses in the Group 5 Data sheet were collected in a real survey. The Codebook labels the respondent sequence and optional contextual comments as synthetic; those labels were not treated as descriptions of the numerical responses. Identifiers were used to check record uniqueness, and contextual text was excluded. Documentation of recruitment and provenance remains the research team's responsibility.

All records contain affirmative consent, adult-eligibility and AI-awareness responses. The sample includes 242 law students, 71 law graduates, 42 advocates or legal professionals and 30 other relevant respondents. It is therefore not a students-only dataset, nor can it be assumed to represent university students across Bangladesh. The supplied materials do not document a probability sampling frame, fieldwork dates, invitation denominator or response rate. The observed N = 385 is not represented as proof of a documented a priori sample-size calculation or population margin of error.

3.2 Measures and analytical roles

Table 1 identifies the two outcomes, four focal awareness items and contextual verification item. The five-point scale runs from strongly disagree to strongly agree. Exact wording is reproduced in Appendix A. DPA2 and DPA3 describe self-reported practices; DPA1, DPA4, AIL1 and AIL3 describe self-reported understanding. AIL2, concerning verification of important AI information, is a contextual covariate rather than an outcome. No item is presented as an objective test of knowledge or behaviour.

Table 1. Measurement content and analytical roles

Code	Abbreviated content	Role
DPA2	Avoids sensitive personal input	Outcome 1
DPA3	Checks privacy information	Outcome 2
DPA1	Recognises privacy risks from input	Focal H1
DPA4	Understands potential processing	Focal H2
AIL1	Recognises plausible inaccuracies	Focal H3
AIL3	Recognises bias or incomplete data	Focal H4
AIL2	Verifies important AI information	Adjustment

Source: Group 5 Codebook. Appendix A gives exact wording. Items record self-reported understanding and practices, not verified knowledge or observed actions.

The mixed content of DPA items makes a single reflective scale difficult to justify without additional validation. The analysis does not report outer loadings, AVE, HTMT or structural paths for unmeasured constructs. It treats the items as distinct indicators and reports their full distributions. This choice follows the principle that content and measurement assumptions require evidence, rather than relying on an attractive model diagram alone.[16]

3.3 Data screening and covariates

The audit checks all 20 agreement items for missingness and permitted values, duplicate identifiers, repeated full item-response vectors and responses uniform across all 20 items. Nine entries in the optional AI-tool field are missing; this field is not used in the models. The experience and frequency fields include conflicting never-use and non-never-use responses. All records remain in the primary analysis because focal items are complete. A sensitivity model retains only respondents reporting non-never values in both experience and frequency fields; this is a usage-restricted subset, not a correction of all possible data-quality issues.

[16] Godfred O Boateng and others, 'Best Practices for Developing and Validating Scales for Health, Social, and Behavioral Research: A Primer' (2018) 6 Frontiers in Public Health 149; Adamantios Diamantopoulos and Heidi M Winklhofer, 'Index Construction with Formative Indicators: An Alternative to Scale Development' (2001) 38 Journal of Marketing Research 269.

The four awareness items and AIL2 enter each model linearly per agreement point, centred at neutral. Additional covariates are any AI training versus none, AI-use frequency coded zero to four, and age 27 or above versus younger. Frequency and agreement coding impose equal-step assumptions. A further sensitivity model adds law-student status. These variables provide an adjusted descriptive specification; they are not a demonstrated causal adjustment set.

3.4 Descriptive and paired analyses

For each analytical item, the study reports category counts, mean, sample standard deviation and endorsement at agree or strongly agree, with pointwise 95% Wilson intervals. A mean summarises numerical coding rather than proving that categories are psychologically equidistant. With unknown sampling probabilities, intervals do not establish representativeness of a wider population.[17]

Three paired contrasts are analysed: DPA3 minus DPA2, DPA1 minus DPA4, and DPA1 minus DPA2. Exact McNemar tests use discordant pairs; Holm correction covers the three tests. Pointwise percentile intervals for percentage-point differences use 10,000 whole-record bootstrap resamples with seed 20261026. The comparison of risk understanding and avoidance is not a test of an attitude–behaviour paradox because wording and referents differ and both responses are self-reported.[18]

3.5 Ordinal regression and paired coefficients

Two proportional-odds models estimate associations with higher responses on DPA2 and DPA3. DPA2 has one category-one response and DPA3 has none, so categories one and two are combined as disagreement for both models. The original five-category distributions remain in the descriptive tables. Each model includes eight slopes and three thresholds. Under logit $\Pr(Y \leq k \mid X) = \alpha k - X\beta$, $\exp(\beta)$ is the common odds ratio for a higher response per unit of a predictor.[19]

Maximum likelihood uses analytic scores, a numerical observed Hessian and HC1 sandwich covariance with factor $N/(N - 11)$. A second optimiser checks coefficients. A cumulative-logit diagnostic compares slopes across the three cutpoints with record-level covariance; its joint test has 16 degrees of freedom. A non-significant diagnostic does not prove exact proportionality. Maximum variance inflation is also assessed.[20]

Holm correction covers the eight focal awareness coefficients across two outcomes. The difference between corresponding DPA3 and DPA2 coefficients is estimated using per-record

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

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

[19] Peter McCullagh, 'Regression Models for Ordinal Data' (1980) 42 Journal of the Royal Statistical Society Series B 109.

[20] Leonard A Stefanski and Dennis D Boos, 'The Calculus of M-Estimation' (2002) 56 American Statistician 29; Rollin Brant, 'Assessing Proportionality in the Proportional Odds Model for Ordinal Logistic Regression' (1990) 46 Biometrics 1171.

influence vectors to preserve paired-outcome covariance. Four coefficient differences receive a joint Wald test and separate Holm-adjusted comparisons. Ratios of odds ratios describe differences between model slopes, not changes in percentage-point endorsement. Pointwise intervals do not incorporate Holm adjustment.[21]

3.6 Sensitivity and reporting

The ordinal models are refitted after adding student status and in the non-never-use subset. Binary models also examine endorsement versus lower responses and strong agreement versus all lower responses. These are different outcome thresholds and are descriptive sensitivity analyses, not new confirmatory tests. Binary estimates are cross-checked with an independent implementation. No imputation or automatic stepwise selection is used. The models cannot address unknown recruitment selection or unrecorded clustering.

3.7 Ethics and participant protection

Ethical approval for this study was obtained from the Center for Academic & Professional Career Development and Research (CAPCDR), an external institutional body, under approval reference CAPCDR: SMUCT/LLB/SS-0020260912-05. External ethical review was sought because Shanto-Mariam University of Creative Technology does not have an institutional ethics committee responsible for reviewing this type of research.

The reported safeguards comprise information about the study, informed consent before completion, voluntary participation, an opportunity to discontinue, an anonymous questionnaire and aggregate reporting. The analysed records contain affirmative consent and adult-eligibility responses. The optional contextual-text field was excluded; individual narratives are not reproduced. Data sharing is subject to confidentiality and applicable institutional requirements. The authors' declarations appear in Section 8.

4. Results

The results separate sample characteristics, item distributions, within-person comparisons and adjusted associations. The two protective-practice outcomes are analysed independently and compared directly. Their different wording must remain visible when interpreting differences. All primary results use N = 385; the usage-restricted sensitivity sample is identified separately.

4.1 Sample and data audit

Table 2 provides the complete recorded profile. Law students make up 62.9% of records, law graduates 18.4%, advocates or legal professionals 10.9%, and other relevant respondents 7.8%. These categories describe current status as recorded, not a nationally representative sample. Education level and current status are distinct fields.

[21] Holm (n 18); Ronald L Wasserstein and Nicole A Lazar, 'The ASA Statement on p-Values: Context, Process, and Purpose' (2016) 70 American Statistician 129.

Table 2. Complete respondent profile

Characteristic	Recorded categories and counts
Age	21-23: 163; 24-26: 81; 18-20: 64; 27-30: 44; 31+: 33
Gender	Male: 200; Female: 173; Prefer not to say: 7; Other: 5
Current status	Law student: 242; Law graduate: 71; Advocate or legal professional: 42; Other relevant respondent: 30
Education	Undergraduate: 216; Graduate: 84; Professional: 43; Postgraduate: 42
Location	Dhaka: 166; District town: 86; Other city corporation: 74; Upazila-rural area: 55; Other: 4
AI experience	1-2 years: 133; 6-12 months: 110; Less than 6 months: 69; More than 2 years: 53; Never: 20
AI frequency	Weekly: 154; Daily or almost daily: 121; Monthly: 64; Less than monthly: 31; Never: 15
AI training	No: 225; Yes, short orientation: 106; Yes, course or certified training: 54

N = 385. Categories sum to 385 within each field. Current status and education level are separate measures; the sample is not restricted to students.

Dhaka accounts for 166 respondents (43.1%), with other recorded locations also represented. All 20 agreement items are complete and within the allowed range. There are no duplicate identifiers, repeated full 20-item vectors or records with the same answer to all 20 items. These checks describe observable properties of the workbook and cannot independently establish participant independence or survey provenance.

4.2 Awareness and reported practices

Table 3 shows the complete original response distributions for DPA1–DPA5. Risk understanding is endorsed by 275 respondents (71.4%). Processing understanding is endorsed by 177 (46.0%), with 162 neutral responses. Checking privacy information is endorsed by 284 (73.8%), while avoidance of sensitive input is endorsed by 222 (57.7%). The user-information expectation in DPA5 is endorsed by 198 (51.4%).

Table 3. Privacy awareness and reported practice distributions

Item	Mean (SD)	Counts 1 / 2 / 3 / 4 / 5	Endorsed n (%)	95% CI %
DPA1	3.95 (0.77)	0 / 8 / 102 / 178 / 97	275 (71.4%)	66.7–75.7
DPA2	3.65 (0.79)	1 / 21 / 141 / 171 / 51	222 (57.7%)	52.7–62.5
DPA3	3.95 (0.79)	0 / 15 / 86 / 189 / 95	284 (73.8%)	69.2–77.9
DPA4	3.43 (0.86)	5 / 41 / 162 / 138 / 39	177 (46.0%)	41.1–51.0
DPA5	3.53 (0.79)	2 / 28 / 157 / 159 / 39	198 (51.4%)	46.4–56.4

N = 385. Categories: 1 strongly disagree; 2 disagree; 3 neutral; 4 agree; 5 strongly agree. Endorsement = 4 or 5. Intervals are pointwise Wilson intervals; means summarise numerical coding.

These responses should not be translated into verified knowledge or observed acts. DPA3, for example, asks whether the respondent checks information before sensitive tasks, not whether a researcher observed the check or assessed the information's quality. DPA2 concerns a public AI tool and sensitive personal information; it is not a general measure of every disclosure practice.

Table 4 reports the three broader AI-literacy items included in the models. Inaccuracy awareness is endorsed by 172 (44.7%), verification practice by 268 (69.6%) and bias awareness by 303 (78.7%). Their different frequencies underline why an overall AI-awareness score would hide important content differences.

Table 4. Broader AI awareness and verification responses

Item	Mean (SD)	Counts 1 / 2 / 3 / 4 / 5	Endorsed n (%)	95% CI %
AIL1	3.41 (0.83)	2 / 44 / 167 / 137 / 35	172 (44.7%)	39.8–49.7
AIL2	3.87 (0.77)	0 / 12 / 105 / 189 / 79	268 (69.6%)	64.8–74.0
AIL3	4.06 (0.78)	0 / 12 / 70 / 185 / 118	303 (78.7%)	74.3–82.5

N = 385. Categories: 1 strongly disagree; 2 disagree; 3 neutral; 4 agree; 5 strongly agree. Endorsement = 4 or 5. Intervals are pointwise Wilson intervals; means summarise numerical coding.

AIL1 concerns the plausibility of inaccurate output, whereas AIL3 concerns bias or incomplete data. Neither is a direct measure of privacy knowledge. Their associations with the two practices are therefore interpreted as exploratory relationships between reported responses.

4.3 Paired comparisons and configurations

Table 5 reports three within-person contrasts. Checking privacy information exceeds avoidance by 62 endorsements, a difference of 16.1 percentage points (95% bootstrap interval 9.6–22.6; Holm-adjusted $p < .001$). The discordant counts are 115 checking-only and 53 avoidance-only endorsements. Risk understanding exceeds processing understanding by 25.5 points, and it

exceeds avoidance by 13.8 points. All three paired tests remain below .001 after Holm adjustment.

Table 5. Paired endorsement differences

Contrast	First only / second only	Difference pp	95% CI pp	Holm p
DPA3 − DPA2	115 / 53	16.1	9.6–22.6	< .001
DPA1 − DPA4	147 / 49	25.5	18.7–31.9	< .001
DPA1 − DPA2	109 / 56	13.8	7.5–20.0	< .001

N = 385; pp = percentage points. Exact McNemar tests with Holm correction across three contrasts. Pointwise percentile intervals use 10,000 whole-record bootstrap resamples. Different statements do not represent a forced-choice task.

The contrasts concern distinct statements, not randomly assigned interventions. The difference between risk understanding and avoidance does not establish a privacy paradox or conscious inconsistency. Neutral responses are included among non-endorsements, and the items refer to different activities. The intervals are pointwise rather than simultaneous intervals for all three comparisons.

Table 6 shows the joint configuration for the two practices. Both are endorsed by 169 respondents (43.9%); 53 (13.8%) endorse avoidance only; 115 (29.9%) endorse checking only; and 48 (12.5%) endorse neither. These four cells sum to 385.

Table 6. Joint endorsement of avoidance and checking

Configuration	Count and percentage
Both avoidance and checking	169 (43.9%)
Avoidance only	53 (13.8%)
Checking only	115 (29.9%)
Neither item endorsed	48 (12.5%)

N = 385. Rows sum to 385. Non-endorsement includes neutrality; these descriptive configurations are not validated respondent types.

The joint table shows substantial overlap alongside the difference in marginal endorsement. It does not establish stable behavioural types. A checking-only response can include neutrality about avoidance, and the questionnaire does not identify why respondents answered the two questions differently.

4.4 Adjusted ordinal associations

The common-slope diagnostic yields $\chi^2(16) = 18.92$, $p = .273$ for avoidance and $\chi^2(16) = 21.94$, $p = .145$ for checking. Maximum variance inflation is 1.10, and the second optimiser agrees within 0.000001 on fitted parameters. These diagnostics support a stable ordinal summary

under the chosen specifications; they do not guarantee correct model specification or causal interpretation.

Table 7 presents the eight focal coefficients and their Holm-adjusted p-values. The smallest adjusted p-value is .515. For avoidance, inaccuracy awareness has an odds ratio of 1.24 with a pointwise 95% interval of 0.99–1.54; the other focal intervals also span one. For checking, all four focal intervals span one. The models therefore provide limited evidence that these specific awareness responses distinguish reported practices after adjustment and multiplicity control.

Table 7. Focal associations with reported protection practices

Awareness item	Avoidance OR (95% CI)	Holm p	Checking OR (95% CI)	Holm p
Privacy-risk awareness	1.15 (0.90–1.46)	1.000	1.13 (0.89–1.44)	1.000
Processing awareness	1.11 (0.87–1.40)	1.000	1.15 (0.93–1.41)	1.000
Inaccuracy awareness	1.24 (0.99–1.54)	0.515	0.99 (0.78–1.25)	1.000
Bias awareness	1.03 (0.80–1.34)	1.000	1.03 (0.78–1.38)	1.000

N = 385. Proportional OR per agreement point for a higher outcome response. Both models include all four awareness items, verification, training, frequency and age. Outcomes pool categories 1–2. Pointwise HC1 intervals; Holm correction across eight focal coefficients.

This finding is not proof that awareness and behaviour are unrelated. The intervals retain a range of possible associations, and the items are self-assessments. McFadden pseudo-R^2 values are .013 for avoidance and .011 for checking. These likelihood-based measures indicate limited improvement over threshold-only models, not a percentage of variance explained.

Figure 2 displays the four focal associations with both reported practices, including their pointwise intervals.

Figure 2. Awareness associations with reported avoidance and checking. Pointwise 95% HC1 intervals; eight focal coefficients are Holm-adjusted.

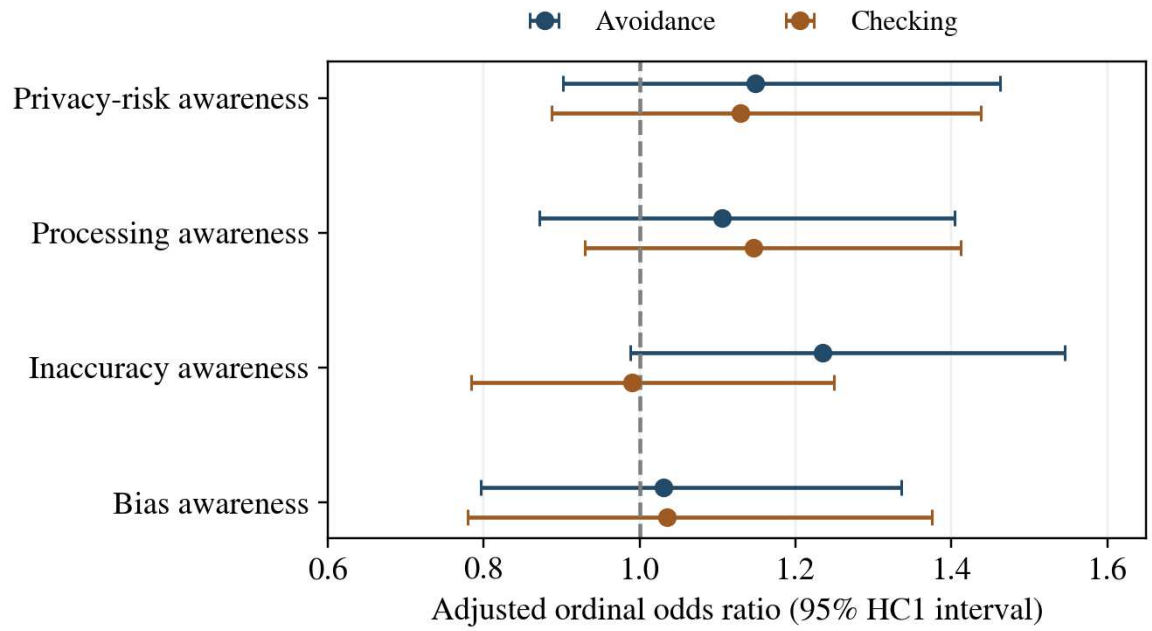


Figure 2 displays the four focal associations with both reported practices

The intervals describe the fitted models and do not themselves incorporate the Holm correction applied to the eight p-values.

Table 8 reports contextual coefficients. General verification practice has a checking odds ratio of 1.29 (95% pointwise interval 1.00–1.65), whereas its avoidance interval spans one. This covariate was not part of the focal eight-test family and its result is descriptive. Training, frequency and age estimates also have intervals spanning one in both models.

Table 8. Contextual coefficients in the ordinal models

Contextual variable	Avoidance OR (95% CI)	Checking OR (95% CI)
Verification practice	1.06 (0.81–1.38)	1.29 (1.00–1.65)
Any AI training	1.23 (0.83–1.83)	1.08 (0.72–1.62)
AI frequency category	1.11 (0.92–1.34)	1.08 (0.86–1.36)
Age 27+	1.27 (0.80–2.02)	1.17 (0.72–1.88)

N = 385. Verification is per agreement point; training compares any with none; frequency is per coded category; age compares 27+ with younger. Pointwise HC1 intervals are descriptive and outside the focal family.

The near-boundary checking interval should not be treated as confirmation that verification causes checking. It reflects concurrent self-reported practices and may share wording or

unmeasured influences with the outcome. A later study could measure their temporal order and perform observed tasks.

4.5 Comparison across practices and sensitivity

Table 9 compares focal coefficients directly between checking and avoidance, retaining their within-record covariance. The joint Wald test is $\chi^2(4) = 1.83$, $p = .768$. All four pointwise ratio intervals include one, and adjusted p-values range from .719 to 1.000. The data do not provide clear evidence that the four awareness-association patterns differ across the two reported practices.

Table 9. Direct comparison of associations across practices

Awareness item	Checking / avoidance OR ratio (95% CI)	Holm p
AI privacy-risk awareness	0.98 (0.69–1.41)	1.000
Data processing awareness	1.04 (0.75–1.43)	1.000
Inaccuracy awareness	0.80 (0.58–1.11)	0.719
Bias awareness	1.00 (0.68–1.48)	1.000

N = 385. Ratios exponentiate checking minus avoidance log-odds coefficients. Paired record-level influence covariance; pointwise intervals; Holm adjustment across four comparisons. Joint Wald $\chi^2(4) = 1.83$, $p = .768$.

This comparison does not establish equivalence. A non-significant difference may reflect limited precision. It is also more informative than asserting a difference solely because one separate model's coefficient has a smaller p-value.

Table 10 presents the student-status-adjusted and usage-restricted ordinal models. The restricted analysis contains 351 records with non-never responses in both usage fields. These estimates have similar magnitudes overall and remain descriptive. The binary threshold analyses show a pointwise association between inaccuracy awareness and strong avoidance, but it is not treated as a separate confirmed discovery; the pointwise interval and changed threshold require caution.

Table 10. Sensitivity of focal ordinal estimates

Specification	Awareness	Avoidance OR (95% CI)	Checking OR (95% CI)
Student status added	Privacy risk	1.15 (0.90–1.46)	1.13 (0.89–1.44)
	Data processing	1.11 (0.87–1.41)	1.15 (0.93–1.41)
	Inaccuracy	1.24 (0.99–1.55)	0.99 (0.78–1.25)
	Bias awareness	1.03 (0.79–1.34)	1.03 (0.78–1.38)
Non-never use	Privacy risk	1.15 (0.89–1.48)	1.12 (0.87–1.44)
	Data processing	1.14 (0.89–1.45)	1.08 (0.87–1.34)
	Inaccuracy	1.20 (0.95–1.53)	1.04 (0.82–1.32)
	Bias awareness	1.00 (0.76–1.32)	1.03 (0.77–1.39)

Student-status-added models: N = 385. Non-never-use models: n = 351, retaining records with non-never values in both experience and frequency fields. Pointwise HC1 intervals; sensitivity estimates are descriptive.

The evidence supports a descriptive separation between reported checking and avoidance, while adjusted relationships between the selected awareness items and the two practices remain uncertain. No estimated coefficient demonstrates an effect of teaching AI awareness or a change in actual disclosure behaviour.

5. Discussion

The findings highlight both differences between reported practices and uncertainty about their relationship with self-reported awareness. More respondents endorsed checking privacy information before sensitive tasks than avoiding sensitive input in public AI tools. More also endorsed a general understanding of privacy risk than an understanding of collection, storage or processing. These are meaningful distinctions in questionnaire responses, but they are not direct evidence that awareness produces or fails to produce protective action.

5.1 Checking and avoidance as different practices

The 16.1-point paired difference suggests that checking and avoidance should not be treated as interchangeable measures. One possible explanation is that respondents consider consulting information compatible with continuing a sensitive task, whereas avoidance means withholding particular content from a public tool. Another is that the items evoke different contexts or standards of behaviour. The survey does not measure these reasons. Follow-up interviews or a controlled vignette could investigate how participants interpret each statement.

The result connects with privacy literacy research by showing why the specific action matters. Studies of online privacy describe multiple ways of managing information, and a general label

such as “protection behaviour” can conceal distinctions between reading, withholding and changing settings. The present data extend this question to an AI-related survey context but do not replicate a behavioural experiment.[22]

The joint configuration also prevents a simplistic interpretation. A substantial group endorses both practices, and the checking-only group includes respondents who are neutral as well as those who disagree with avoidance. Calling this group careless or describing it as rejecting privacy would go beyond the responses. The stronger conclusion is that the two self-reported items generate different distributions and merit separate measurement.

5.2 Risk recognition and processing understanding

The 25.5-point difference between general risk understanding and processing understanding invites a more precise educational question. A general statement that information entered into AI may create risk does not require a respondent to describe what collection, storage or processing means. The lower endorsement of DPA4 may reflect uncertainty about those operations, but the survey does not test actual knowledge and cannot identify the cause. The two questions also differ in wording, so their difference is not a measured learning deficit.

For education, the relevant next step is to specify the service and activity. A learner could examine a real notice, identify the information collected and distinguish account-specific settings from general statements. An assessment could then ask what the learner would disclose for a defined task. Such a design would measure understanding rather than only confidence in understanding. UNESCO’s education guidance and research on online privacy literacy support considering both user capability and institutional arrangements.[23]

5.3 Interpreting the adjusted findings

None of the eight focal awareness coefficients remains distinguishable from zero after Holm adjustment. This limits support for the proposed response associations in the fitted models. It does not demonstrate that privacy education has no value or that all potentially relevant effects are negligible. The intervals are compatible with a range of associations, and the survey does not contain objective awareness measures, observed behaviour or an intervention.[24]

The direct comparison between outcome-specific coefficients is similarly inconclusive. The paired covariance is necessary because the same respondents supplied both outcomes, and the joint test addresses whether the four slopes differ as a set. A non-significant joint test does not prove equal effects. It also does not erase the descriptive difference between the item endorsement rates: marginal distributions and adjusted associations answer different questions.

The strong-avoidance sensitivity estimate for inaccuracy awareness is another reason to keep thresholds distinct. It uses only the strongly agreeing group and yields a pointwise interval that differs from the ordinal summary. This analysis was not assigned a new confirmatory family.

---

[22] Baruh, Secinti and Cemalcilar (n 3); Barth and de Jong (n 4).

[23] Miao and Holmes (n 1); Baruh, Secinti and Cemalcilar (n 3).

[24] Wasserstein and Lazar (n 21); Douglas G Altman and J Martin Bland, ‘Absence of Evidence Is Not Evidence of Absence’ (1995) 311 BMJ 485.

Selecting it because it crosses a nominal threshold would understate the uncertainty created by multiple comparisons and specification choices.[25]

5.4 Theoretical interpretation

Privacy calculus suggests that people consider several factors when deciding whether to disclose information, including perceived benefits and trust as well as risk. The present questionnaire does not measure the full calculus for a particular task. Its findings therefore neither validate nor invalidate the theory. They identify potential inputs and outcomes for a future study that measures benefits, risk, alternatives and an actual disclosure choice independently.[26]

Protection motivation theory similarly directs attention to coping appraisal as well as threat appraisal. The weak adjusted findings are compatible with the possibility that a person who recognises risk may still find a protective step difficult, ineffective or costly, but the survey does not measure those explanations. Future studies could ask whether users believe a specific action will work and whether they can perform it.[27]

The theory of planned behaviour adds attitudes, social expectations and perceived control to the research agenda. These constructs were not measured as a complete model. The present contribution is a measurement argument: retaining distinct awareness and practice items allows each relationship to be examined without presenting a general theory as confirmed by item labels.[28]

5.5 Bangladesh context and study limits

The existing Personal Data Protection Act 2026 provides a legal setting for discussions of access, correction, transparency and security. Its application to a specific AI service depends on facts and relevant legal provisions. Survey respondents were not asked to demonstrate legal knowledge or identify a provider's compliance. The article's recommendations therefore focus on practical questions for education and governance rather than claiming that participants have established a breach.[29]

The sample includes a substantial law-student group as well as graduates and professionals. It offers a view of the recorded respondents, not a national estimate for all university students. The absence of documented recruitment procedures and fieldwork dates limits assessment of selection. All focal answers are self-reported and collected in one cross-section, and no information establishes the timing of awareness relative to practice. These limits shape the interpretation rather than disqualifying the descriptive findings.

---

[25] Holm (n 18); Wasserstein and Lazar (n 21).

[26] Dinev and Hart (n 7).

[27] Rogers (n 8).

[28] Ajzen (n 9); Boateng and others (n 16).

[29] Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 11; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 15; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 17.

A subsequent study should distinguish actual student status, field of study and service experience; document the sampling and recruitment process; and test comprehension using specific privacy disclosures. Observed choices in simulated tasks, followed by interviews, could clarify whether participants understand a notice and how they act on it. A randomised educational intervention with baseline and follow-up measurements would be needed to evaluate whether increased awareness causes a change in practice.

6. Theoretical and Practical Implications

The results suggest that privacy education and AI governance should recognise several distinct points in a user's decision: awareness of a potential risk, understanding of data processing, consultation of information and a choice about what to enter. These steps may be connected, but the present survey does not establish a causal sequence. The implications are therefore prospective recommendations for measurement and institutional design, grounded in the item-level findings and the cited literature.

6.1 Theoretical implications

The study supports treating awareness as multidimensional at the level of content. General privacy-risk understanding, awareness of data processing, recognition of inaccurate outputs and awareness of bias concern different matters. The two self-reported practices also differ. A model that combines them without evidence of dimensionality could mask meaningful relationships or create artificial correlations. Future measurement work should test whether items reflect common constructs and should distinguish subjective confidence from verified knowledge.[30]

The privacy calculus and protection motivation perspectives can be brought together in a later study if their components are measured independently. Perceived benefits and risks could be examined alongside coping efficacy, available alternatives and an observed decision. The current data cannot establish such an integrated mechanism, but they identify why an assumption that awareness alone drives protection needs testing.[31]

The comparison across outcomes also has a methodological implication. Different significance levels in two regressions do not demonstrate that their associations differ. The paired coefficient comparison directly examines that question and retains within-respondent covariance. Its inconclusive result should be used to plan a better-powered study with more precise measures, not to assert equivalence between practices.[32]

6.2 Educational and institutional implications

Universities can teach students how to identify the data involved in an AI task, distinguish sensitive from non-sensitive content, locate applicable service information and assess whether an alternative is available. Practical exercises should ask learners to explain a specific notice and make a decision about a realistic document. This goes beyond telling users to "be aware"

[30] Boateng and others (n 16); Diamantopoulos and Winklhofer (n 16).

[31] Dinev and Hart (n 7); Rogers (n 8).

[32] Altman and Bland (n 24); Wasserstein and Lazar (n 21).

and creates an opportunity to evaluate comprehension. The study's reported practices offer a reason to test such teaching, but they do not demonstrate its effectiveness.[33]

Institutions can also review their own use of AI services. Appropriate questions include which tools are approved for sensitive material, whether agreements specify data handling, what settings are available, and where students and staff can obtain guidance. Clear communications should identify both the permitted task and the limits of the institution's knowledge about the service. A user's agreement that they check privacy information does not itself establish that the information is accessible or sufficient.

For policymakers and service providers, transparent information and usable rights mechanisms are complementary to individual training. The cited Bangladeshi Act addresses access, correction, transparency and security subject to its scope and implementation. The survey does not establish whether any provider meets those requirements. Future assessment should connect the legal text to actual service practices and affected users, rather than relying on a general attitude score.[34]

7. Conclusion, Limitations and Future Research

This study analysed 385 adult, AI-aware survey records in Bangladesh to examine awareness and self-reported personal-data protection practices. Checking privacy or data-use information was endorsed by 73.8% and avoiding sensitive input in public AI tools by 57.7%, a paired difference of 16.1 percentage points. General privacy-risk understanding was endorsed more often than understanding of collection, storage or processing. The items differ in scope and wording, so these descriptive differences are not causal effects or proof of a privacy paradox.

The adjusted ordinal models offered limited evidence for the eight proposed awareness–practice associations after Holm correction. A paired comparison of the four association patterns across the two practices was inconclusive. These results do not establish that awareness is unimportant, and they do not show that it improves or worsens actual disclosure decisions. Their principal contribution is to distinguish specific self-reported understandings and actions while preserving uncertainty about their relationships.

The study is limited by a mixed sample dominated by law students, undocumented recruitment and fieldwork details, self-report, single items and a cross-sectional design. The workbook does not establish national representativeness or observe actual AI-service interactions. Formal ethics approval was not obtained; the authors describe their institutional context and participant-protection safeguards in Section 8. The original wording of each analytical item is supplied in Appendix A to support interpretation.

Future research should document recruitment and study people using specified services for defined tasks. Independent knowledge checks, observed disclosure choices and qualitative interviews can identify how participants understand privacy information and what obstacles

[33] Miao and Holmes (n 1).

[34] Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 11; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 12; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 15; Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026), s 17.

they encounter. A controlled educational study with baseline and follow-up measures could test whether particular training or interface changes affect protective decisions. The present analysis provides a transparent starting point by showing where responses differ and where stronger evidence is needed.

Declarations

Ethical approval and oversight

Ethical approval for this study was obtained from the Center for Academic & Professional Career Development and Research (CAPCDR), an external institutional body, under approval reference CAPCDR: SMUCT/LLB/SS-0020260912-05. External ethical review was sought because Shanto-Mariam University of Creative Technology does not have an institutional ethics committee responsible for reviewing this type of research.

Informed consent

Informed consent was obtained from adult participants before questionnaire completion. The questionnaire explained the study purpose, voluntary participation, anonymity and the option to discontinue. All analysed records contain affirmative consent and adult-eligibility responses.

Data availability

The numerical data supporting the reported analyses are held by the research team. Requests for de-identified data and analytical specifications may be directed to the corresponding author. Any sharing is subject to participant confidentiality and applicable institutional requirements. The contextual-text field was excluded from the analysis.

Author contributions

Moumita Akter Mira: Lead student researcher; conceptualisation; preparation of study materials; organisation and curation of survey data; manuscript development. The project was conducted under the supervision of Prof. Dr Kazi Abdul Mannan.

Kazi Abdul Mannan: Conceptual and methodological guidance; supervision; interpretation of statistical findings; critical review and editing of the manuscript.

Generative AI disclosure

Generative AI assisted manuscript drafting, language editing, organisation and the development of analytical code. Statistical estimates were computed programmatically from the numerical survey data. Responsibility for the study's analysis, interpretation and reporting rests with the authors.

Bibliography

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

Altman DG and Bland JM, ‘Absence of Evidence Is Not Evidence of Absence’ (1995) 311 BMJ 485

Bajnaid W and Aljasir S, ‘Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region’ (2025) 6 Journalism and Media 8

Barth S and de Jong MDT, 'The Privacy Paradox: Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review' (2017) 34 Telematics and Informatics 1038
Baruh L, Secinti E and Cemalcilar Z, 'Online Privacy Concerns and Privacy Management: A Meta-Analytical Review' (2017) 67 Journal of Communication 26
Boateng GO and others, 'Best Practices for Developing and Validating Scales for Health, Social, and Behavioral Research: A Primer' (2018) 6 Frontiers in Public Health 149
Bovens M, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13 European Law Journal 447
Brant R, 'Assessing Proportionality in the Proportional Odds Model for Ordinal Logistic Regression' (1990) 46 Biometrics 1171
Diamantopoulos A and Winklhofer HM, 'Index Construction with Formative Indicators: An Alternative to Scale Development' (2001) 38 Journal of Marketing Research 269
Dinev T and Hart P, 'An Extended Privacy Calculus Model for E-Commerce Transactions' (2006) 17 Information Systems Research 61
Dombrowski J and Trepte S, 'Taking Stock of Social Media Privacy: Meta-Analytic Evidence on How Control, Trust, and Concerns Are Associated with Social Media Use, Disclosure, and Protection' (2026) 31 Journal of Computer-Mediated Communication zmaf025
Efron B and Tibshirani RJ, *An Introduction to the Bootstrap* (Chapman & Hall 1993)
Holm S, 'A Simple Sequentially Rejective Multiple Test Procedure' (1979) 6 Scandinavian Journal of Statistics 65
McCullagh P, 'Regression Models for Ordinal Data' (1980) 42 Journal of the Royal Statistical Society Series B 109
McNemar Q, 'Note on the Sampling Error of the Difference between Correlated Proportions or Percentages' (1947) 12 Psychometrika 153
Miao F and Holmes W, *Guidance for Generative AI in Education and Research* (UNESCO 2023) <https://doi.org/10.54675/EWZM9535> accessed 27 October 2026
Ng DTK and others, 'Conceptualizing AI Literacy: An Exploratory Review' (2021) 2 Computers and Education: Artificial Intelligence 100041
Podsakoff PM and others, 'Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies' (2003) 88 Journal of Applied Psychology 879
Rogers RW, 'A Protection Motivation Theory of Fear Appeals and Attitude Change' (1975) 91 Journal of Psychology 93
Stefanski LA and Boos DD, 'The Calculus of M-Estimation' (2002) 56 American Statistician 29
Wasserstein RL and Lazar NA, 'The ASA Statement on p-Values: Context, Process, and Purpose' (2016) 70 American Statistician 129
Wilson EB, 'Probable Inference, the Law of Succession, and Statistical Inference' (1927) 22 Journal of the American Statistical Association 209

Appendix A. Analytical item wording

Table A1 reproduces the analytical items from the Group 5 Codebook. The wording distinguishes self-reported understanding from reported practices.

Table A1. Exact analytical item wording

Code	Statement
DPA1	I understand that information entered into an AI system may create privacy risks.
DPA2	I avoid entering sensitive personal information into public AI tools.
DPA3	I check privacy or data-use information before using an AI service for sensitive tasks.
DPA4	I understand that AI services may collect, store or process user data.
DPA5	I believe users should receive clear information about how their data are used by AI systems.
AIL1	I understand that generative AI can produce plausible but inaccurate information.
AIL2	I verify important AI-generated information before relying on it.
AIL3	I understand that AI outputs may reflect bias or incomplete data.

Source: Group 5 Codebook. One strongly disagree; two disagree; three neutral; four agree; five strongly agree.

All items use the five agreement categories in the Codebook; none is reverse-coded or combined into a composite in this analysis.

Table of legislation

Personal Data Protection Act 2026 (Bangladesh Act No 63 of 2026)