# Measuring Privacy Literacy on Generative AI: A Pilot Study of Generation Z

Jing Hua
*Dept.of Information Technology*
*La Roche University*
Pittsburgh, USA
jing.hua@laroche.edu

Wenli Wang
*Dept. of Computer Information Systems*
*Robert Morris University*
Moon Township, USA
wangw@rmu.edu

***Abstract*— As generative artificial intelligence systems such as ChatGPT, Gemini, and Midjourney become integral to the digital lives of Generation Z, understanding users' privacy literacy is essential for improving AI platform transparency and usability. This study proposes the DCPS (Declarative, Cognitive and Procedural Score) framework to assess AI privacy literacy. The DCPS framework measures privacy literacy in three dimensions: Declarative Knowledge (factual understanding of data practices), Cognitive Knowledge (evaluation of privacy risk, control, and trust), and Procedural Knowledge (practical skills in managing privacy settings) and establishes a 0-10 composite score indicating total privacy literacy. A pilot study of 73 university students provided an empirical baseline for Generation Z's AI privacy literacy. Results show low declarative knowledge and cognitive awareness of privacy risks, but very low procedural competence, revealing a substantial gap between awareness and action. The DCPS privacy literacy framework in AI contexts provides valuable guidance to help improving transparency, user education, and privacy-centered design in generative AI systems.**

***Keywords—Generative AI, Privacy Literacy, DCPS Framework, Large Language Models, User Awareness, Data Privacy, Human - AI Interaction, Usability, Generation Z***

## I. Introduction

Since the public release of ChatGPT in late 2022, generative artificial intelligence (GenAI) tools have rapidly diffused across educational and professional settings, with university students representing one of the largest early adopter groups [1]. This demographic trend has led to a surge in research on AI literacy, focusing on users' knowledge, skills, and attitudes toward AI technologies [2]. However, AI literacy does not necessarily equate to privacy literacy, as understanding how AI functions is distinct from knowing how to manage personal data responsibly [3][4].

Recent reports highlight a persistent awareness and behavior gap among generative AI users. The Cisco 2024 Consumer Privacy Survey found that 30% of users enter personal or confidential information into generative AI tools, despite 84% expressing concerns about the potential public exposure of such data [5]. Similarly, Ng et al. (2025) analyzed generative AI usage guidelines from universities worldwide and found that privacy and security are inconsistently defined and often delegated to individual responsibility [2]. They emphasized the need for clearer institutional guidance and stronger privacy literacy among students and staff to ensure responsible AI use in higher education. Within the current wave of AI adoption, examining privacy literacy among generative AI users, particularly university students, offers critical insight into whether awareness translates into responsible behavior. As Zhang et al. (2021) have noted, developing appropriate digital and ethical behavior is essential to mitigate the unintended social consequences of AI technologies [6]. Similarly, Hua and Wang (2025) emphasize that strong digital competence alone does not guarantee privacy-protective behavior, underscoring the need to integrate ethical and privacy considerations into digital literacy education [7]. Within the current wave of AI adoption, examining privacy literacy among generative-AI users—particularly university students—offers critical insight into whether awareness translates into responsible behavior. As early adopters, Generation Z's practices provide an indicative snapshot of public engagement with AI privacy controls and policies.

Understanding how Generation Z users perceive and manage privacy in generative AI environments is significant for both research and design. As digital natives and early adopters, this group's behaviors provide early evidence of how the public may engage with AI privacy controls and policies. By examining their literacy levels, this study contributes empirical insights to guide AI usability design, policy transparency, and privacy education. Specifically, it proposes the DCPS (Declarative, Cognitive, Procedural Score) framework to conceptualize and measure privacy literacy, applicable to AI. The remainder of this paper presents the theoretical foundation of the framework, describes the framework, applies the framework in a pilot study of Generation Z, and discusses implications for future research and responsible AI development.

## II. Literature Review

Current research on AI digital literacy often classifies privacy literacy as part of the broader ethical dimension of digital competence frameworks [15]. However, this aspect remains underexplored and inconsistently operationalized. Prior studies show that strong general digital literacy does not necessarily correspond to strong privacy literacy [3][4][7][10]. Individuals may demonstrate technical proficiency and awareness of AI tools yet lack understanding of how those systems collect, process, and share personal data.

Prior research defines privacy literacy as the understanding of data collection practices, privacy laws, and associated risks as well as the practical skills of managing privacy settings and using protection tools [3][4][10]. Evidence suggests that individuals often underestimate the visibility and sharing of their data, limiting their abilities to adopt effective privacy measures [7][8][9][10].

Two main approaches have been used to conceptualize privacy literacy. The first distinguishes between declarative knowledge ("know what") and procedural knowledge ("know how") [7][16]. The second expands this view to include a third component, understanding risks, then integrating a cognitive or evaluative dimension [4][10]. Prior studies, however, have focused primarily on self-reported awareness or perceived control rather than empirically measuring factual understanding. This limitation constrains the precision and comparability of privacy literacy assessments across contexts.

Research on students' perceptions of AI use in education shows that most students are open to using GenAI and view it as a learning assistant or tutoring tool [11][12]. However, only a small proportion expressed concerns about overreliance and data privacy violation [12]. Much of the existing literature on AI literacy focuses on the development of AI-related knowledge, skills, and attitudes, often emphasizing educational design and competency measurement rather than privacy understanding [13][14][15]. For instance, Ng et al. (2024) developed the ABCE model, where privacy is included only as part of the ethical dimension alongside security, social responsibility, and digital rights [15]. Similarly, Carolus et al. (2023) and Mansoor et al. (2024) highlighted ethical awareness and responsible AI use but provided limited empirical focus on users' understanding of data practices [13][14].

These findings suggest that while AI literacy education aims to cultivate responsible AI engagement, privacy literacy remains conceptually embedded within broader ethical or digital-responsibility frameworks and is rarely examined as an independent construct. Moreover, privacy literacy is highly contextual, varying by users' familiarity, platform policies, and transparency of data practices [7]. This gap underscores the need for empirical studies exploring users' conceptual and practical understanding of data privacy in generative AI contexts, particularly among Generation Z, the digital natives most actively engaging with GenAI tools. The next section elaborates on the design of the DCPS framework.

## III. The DCPS Privacy Literacy Framework

Building on earlier research assessing privacy literacy in e-commerce [7][17], this study extends the privacy literacy research to generative AI contexts, where large language models (LLMs) such as ChatGPT, Gemini, and Claude exhibit more uniform and publicly documented data-handling policies. This transparency enables systematic evaluation of factual privacy knowledge and facilitates development of a multidimensional measurement model, called DCPS (Declarative, Cognitive, Procedural Score) privacy literacy framework.

### *A. DCPS Privacy Literacy Framework Overview*

The DCPS (Declarative, Cognitive, Procedural Score) framework conceptualizes AI privacy literacy as three interrelated knowledge dimensions that capture what users know, how they reason, and what they do regarding privacy in GenAI environment:

- Declarative: Factual understanding of data practices (e.g., whether and how prompts, uploads, device data, and account information in GenAI are collected, stored, retained, or shared).
- Cognitive: Risk perception and evaluative judgment (e.g., recognizing potential harms, assessing claims about data safety, understanding trade-offs, perceived control, and trust).
- Procedural: Practical skills and behaviors (e.g., finding privacy settings, taking privacy-protective actions, verifying whether changes were successful).

The framework is modular, allowing researchers to emphasize one or more dimensions independently or to aggregate them into a composite privacy literacy score. By combining factual, cognitive, and behavioral competencies, DCPS provides a flexible basis for assessing and comparing AI privacy literacy across user groups and platforms. Table I summarizes the operational structure of the DCPS framework, outlining how each knowledge dimension connects conceptually and empirically to its indicators and overall scoring system.

### *B. Declarative Knowledge of Privacy Literacy*

Declarative Knowledge of privacy literacy (see Table II) addresses what is true about AI data practices. Earlier work often avoided direct factual assessment because platform practices vary by context. In the GenAI domains, public documentation and broadly similar categories of practices (content logging, retention/human review, device/usage, account/financial information, training opt-outs/limits) make consistent factual assessment feasible. This dimension captures the baseline knowledge users bring to evaluating AI privacy risks. Its mean subscale (0-10) contributes to 30% of composite DCPS score.

TABLE I. Contruct Map of DCPS (Declative, Cognitive, Procedural Score) Privacy Literacy Framework

| Dimensions | Core Principle | Conceptual Focus | Operational Variables /Indicators | Score |
|---|---|---|---|---|
| **Declarative Knowledge** | Know What | Factual understanding of data practices | Variables measuring users' factual knowledge of data practices across six categories: prompt/content data, device information, account data, profiling, data retention, and deletion policies and practices. | Subscale 0-10 |
| **Cognitive Knowledge** | Know Why | Evaluation of privacy risk, control, and trust | Variables representing three thematic areas: (a) Risk awareness & safety evaluation, (b) misconception recognition, and (c) perceived control & trust. They reflect users' interpretation and reasoning about privacy risks and data-use practices. | Subscale 0-10 |
| **Procedural Knowledge** | Know How | Practical skills and behaviors for privacy protection | Variables representing awareness of privacy settings, execution of privacy-related actions, and perceived outcomes or success | Subscale 0-10 |
| **DCPS Score** | Know Total | Integrated privacy literacy score | Weighted sum product of the three subscales = Declarative * 0.3 + Cognitive * 0.3 + Procedural * 0.4 | Score 0-10 |

Note: Each of the three DCPS knowledge dimensions can be operationalized through multiple measurable indicators.

TABLE II. DECLARATIVE KNOWLEDGE OF PRIVACY LITERACY

| Declarative Knowledge | Conceptual Examples | Scoring Method |
|---|---|---|
| **Prompt & Content Data** | Understanding that technology products can store user-submitted prompts, files, or outputs. | Evaluated on a 0-10 subscale; Contributes to 30% of DCPS score. |
| **Device & Usage Data** | Awareness that device type, browser, or IP information can be logged. | |
| **Account & Payment Data** | Knowledge that account and payment information can be retained by technology providers. | |
| **Content Profiling & Moderation** | Awareness that technology systems can record content for safety or moderation review. | |
| **Data Retention & Human Review** | Understanding that interactions can be stored or reviewed by human and/or AI moderators. | |
| **Deletion & Product Revision Policies** | Knowledge of data-deletion limits and how user history settings affect product revision. | |

### *C. Cognitive Knowledge of Privacy Literacy*

Cognitive Knowledge of privacy literacy reflects how users perceive and evaluate risk (e.g., potential harms from sharing personal/sensitive data with public GenAI applications), as well as their sense of control/trust. It complements factual knowledge by indicating whether users recognize when a behavior is risky and can critically assess safety claims.

TABLE III. COGNITIVE KNOWLEDGE OF PRIVACY LITERACY

| Cognitive Knowledge | Conceptual Examples | Scoring Method |
|---|---|---|
| **Perceived Risk Awareness** | Recognizing that sharing personal or sensitive data in public GenAI applications may expose privacy risks. | Evaluated on a 0-10 subscale; Contributes to 30 % of DCPS score. |
| **Evaluation of Data Practices** | Understanding that chat histories, deletions, or opt-out settings affect how information is stored and reused by AI providers. | |
| **Recognition of Unsafe Assumptions** | Identifying misconceptions (e.g., believing "temporary chat" prevents company access) and adjusting beliefs accordingly. | |
| **Perceived Control and Trust** | Assessing the extent to which users feel able to manage privacy settings and trust AI platforms' data-use claims. | |
| **Critical Reasoning about Transparency** | Judging whether AI privacy statements and safety disclaimers provide adequate, truthful information. | |

Table III presents the conceptual structure of the Cognitive Knowledge dimension in the DCPS framework. This dimension captures how users evaluate and reason about privacy risks in technological environments. It encompasses awareness of potential harms, recognition of unsafe assumptions, perceptions of control and trust, and the capacity to critically appraise transparency claims. Conceptually, the Cognitive subscale operates on a 0 -10 range and accounts for 30% of the composite DCPS score.

In the pilot study, the cognitive knowledge dimension was operationalized through five evaluative indicators aligned with these three conceptual clusters, capturing users' perception of risk, recognition of misconceptions, and sense of control and trust. Together, these indicators capture how users interpret, judge, and reason about privacy risks when interacting with generative-AI systems.

### *D. Procedural Knowledge of Privacy Literacy*

Procedural Knowledge of privacy literacy covers "knowing how" to act on concerns: finding settings, taking protective steps, and confirming success. It is composed of three subcomponents: awareness of controls, privacy-protective actions and outcome verification (efficacy).

TABLE IV. PROCEDURAL KNOWLEDGE OF PRIVACY LITERACY

| Procedural Knowledge | Conceptual Examples | Scoring Method |
|---|---|---|
| **Awareness of Controls** | Recognizing that AI platform privacy and account-setting options exist and knowing where to locate them. | Evaluated on a 0-10 subscale; Contributes to 40% of DCPS score. |
| **Privacy-Protective Actions** | Demonstrating initiatives to adjust privacy or data-use settings, limit data sharing, or delete stored content. | |
| **Outcome Verification (Efficacy)** | Confirming that intended privacy changes are successfully implemented and understanding their effects. | |

Table IV outlines the conceptual structure of the Procedural Knowledge dimension in the DCPS framework. This dimension reflects the "know how to" aspect of privacy literacy, users' ability to translate awareness and concern into concrete action. It encompasses awareness of available controls, engagement in privacy protective behaviors, and the capacity to verify successful outcomes. The Procedural subscale is expressed on a 0-10 range and carries a slightly higher weight of 40% in the composite DCPS score to emphasize the importance of the most practical behavioral component of privacy competence.

### *E. DCPS Score*

The composite DCPS score is a weighted sum product of the subscales in three knowledge dimensions with proportional weights of 0.3 for Declarative Knowledge, 0.3 for Cognitive Knowledge, and 0.4 for Procedural Knowledge. It emphasizes behavioral literacy, reflecting the practical importance of verifiable action outcome. This weighting aligns with behavioral-change theory, in which knowledge and perception precede action, and ensures high sensitivity to users' applied privacy competence.

## IV. PILOT STUDY

Building on DCPS framework, this pilot study examines Generation Z's privacy literacy baselines in GenAI. It aims to establish a Generation Z's baseline for the three DCPS knowledge dimensions and evaluate the composite DCPS score. It measures how Generation Z users perform across the three DCPS knowledge dimensions - Declarative ("know what"), Cognitive ("assess why or how risky"), and Procedural ("know how") and their composite DCPS scores. It further examines which DCPS dimension demonstrates the weakest baseline among Generation Z users, indicating the greatest need for educational or design interventions.

TABLE V. OPERATIONALIZATION OF DCPS (DECLATIVE, COGNITIVE, PROCEDURAL SCORE) PRIVACY LITERACY FRAMEWORK

| DCPS | Indicators | Examples | Scale | Score | Notes |
|---|---|---|---|---|---|
| **Declarative Knowledge** | 14 factual statements in 6 categories (prompt/content data, device/usage, account, profiling, retention, deletion) | "LLMs store prompts and outputs" "Turning off chat history is a guarantee that nothing is stored" | 5-point Likert | 0-10 | Higher scores indicate greater factual understanding of data practices |
| **Cognitive Knowledge** | 5 attitudinal items on perceived risk, control, and trust | "Entering personal information into an LLM is risky" "Privacy settings provide sufficient control" | 5-point Likert | 0-10 | Higher scores reflect stronger awareness and evaluative reasoning about privacy risks |
| **Procedural Knowledge** | 3 behavioral items measuring awareness of privacy management, privacy actions, and outcome success | "Visited privacy settings" "Disabled chat history" "Successfully made changes" | categorical | 0-10 | Higher scores represent higher competence in performing privacy-protective actions |
| **DCPS Score** | Weighted sum product of three knowledge dimensions' scores: Declarative * 0.3 + Cognitive * 0.3 + Procedural *0.4 | | numerical | 0-10 | Higher scores indicate greater total privacy literacy |

## A. Data Collection

To demonstrate the application of the DCPS framework, a pilot study was conducted with Generation Z participants enrolled in a university. The online survey was administered in class during scheduled sessions to encourage participation and ensure a consistent testing environment. Participation was voluntary, and no personally identifiable information (PII) was obtained.

Following theoretical refinement, the survey items were reorganized according to the DCPS framework. Declarative literacy was assessed through factual indicators of GenAI data handling Cognitive literacy through evaluative reasoning about privacy risk and control, and Procedural literacy through awareness, action, and outcome indicators. Each subscale was standardized on a 0-10 range, with higher values indicating stronger competence. Subscale means were combined into a composite DCPS score using a weighted formula (Declarative * 0.3 + Cognitive * 0.3 + Procedural * 0.4). To clarify how each dimension was operationalized, Table V summarizes the DCPS structure, indicators, and scoring design.

## B. Demogrpahics

A total of 80 students participated in the survey, and among them, 73 provided valid responses. Participation was voluntary, and no personally identifiable information was obtained. Table VI presents the demographic characteristics of the participants, including gender, age, academic level, and field of study. The final sample included undergraduate and graduate students aged 18-30+, representing diverse academic backgrounds and demographic characteristics typical of a Generation Z university cohort. The gender distribution was relatively balanced, with 43.8% male, 49.3% female, and 6.8% preferring not to disclose, supporting generalizability within university populations where gender representation across disciplines is often uneven.

Most participants were within the 18-20 age group (49.3%), followed by 21-23 (21.9%), reflecting the predominance of early undergraduate students. A smaller proportion (13.7%) were aged 24-29, and 4.1% were 30 or older, indicating limited participation from mature or returning students. About 11% chose not to report their age. The age distribution aligns with Generation Z's typical university enrollment profile and situates the study within its target demographic.

The majority were freshmen (42.5%) and sophomores (23.3%), while juniors (13.7%) and seniors (11%) represented smaller cohorts. A small number of graduate students (5.5%) also participated. This composition suggests that most respondents were early in their academic study and possibly at initial stages of exploring generative AI technologies both academically and personally.

Participants represented a broad mix of academic disciplines. Approximately 41% came from computing-related or business fields (Computer Science & IT 15.1%, Information Systems 13.7%, Cybersecurity 12.3%), while 45.2% were enrolled in nontechnical programs such as health, design, or education. This diversity supports cross-disciplinary analysis of privacy literacy and highlights that generative AI adoption extends beyond traditional technology domains.

Overall, the demographic profile indicates a predominantly young, undergraduate, and multidisciplinary Generation Z cohort with balanced gender representation and varied academic exposure to technology. This diversity enhances the study's relevance for examining baseline Gen AI privacy literacy among general student populations rather than highly specialized or technology-only groups.

TABLE VI. PARTICIPANT DEMOGRAPHICS (N = 73)

| Category | Subgroup | Count | Percentage |
|---|---|---|---|
| Gender | Male | 32 | 43.8% |
| | Female | 36 | 49.3% |
| | N/A | 5 | 6.8% |
| Age | 18–20 | 36 | 49.3% |
| | 21–23 | 16 | 21.9% |
| | 24–29 | 10 | 13.7% |
| | 30+ | 3 | 4.1% |
| | N/A | 8 | 11% |
| Academic Level | Freshman | 31 | 42.5% |
| | Sophomore | 17 | 23.3% |
| | Junior | 10 | 13.7% |
| | Senior | 8 | 11% |
| | Graduate (Master/Doctoral) | 4 | 5.5% |
| | N/A | 3 | 4.1% |
| Major | Computer Science/IT | 11 | 15.1% |
| | Information Systems | 10 | 13.7% |
| | Cybersecurity | 9 | 12.3% |
| | Accounting/Finance/ Business | 10 | 13.7% |

| | | | |
|---|---|---|---|
| | Other (Health, Design, Education…) | 33 | 45.2% |

### C. Results

As shown in Table VII the majority (79.4%) reported using free versions of generative-AI platforms, while 11% subscribed to paid plans and 9.6% preferred not to disclose. This reliance on free access may limit exposure to advanced privacy or data-control features, which are often available only in premium accounts. The predominance of younger, early academic-stage students relying on free AI tools provides important context for interpreting DCPS performance across the three knowledge dimensions. Figure 1 complements Table VII by illustrating the distribution of free versus subscription users among participants.

TABLE VII. DISTRIBUTION OF GENERATIVE AI TOOL ACCESS (N = 73)

| | Category | Count (n) | Percentage |
|---|---|---|---|
| **AI Tool Access** | Free version users | 58 | 79.4% |
| | Subscription users | 8 | 11% |
| | Prefer not to say | 7 | 9.6% |

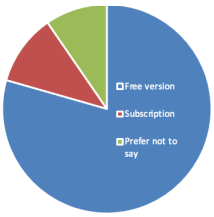


Fig. 1. Distribution of Free vs. Subscription Generative-AI Tool Use

Before assessing privacy literacy, participants were asked which generative-AI tools they used most frequently. A total of 67 valid responses were obtained for this item, as several participants skipped the optional ranking question. As shown in Figure 2, ChatGPT (OpenAI) was by far the most commonly used tool (approximately 85% of respondents), followed by Gemini (Google) (71%) and Claude (Anthropic) (59%). Smaller proportions reported using Perplexity, Copilot, or Midjourney. This distribution provides important context for interpreting DCPS results, as participants' privacy understanding is likely influenced by the data-use and transparency practices of the platforms they engage with most—particularly ChatGPT and Gemini.

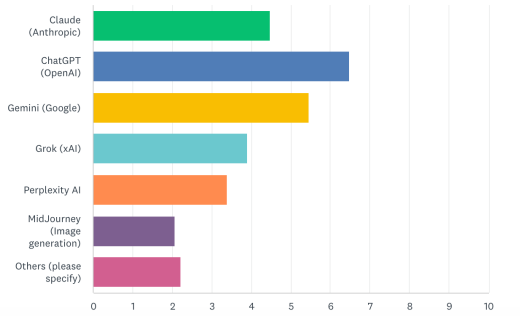


Fig. 2. Popular Generative AI platforms use

Descriptive statistics (Table VIII) indicate variation across the three DCPS dimensions. Generation Z participants demonstrated low factual understanding of GenAI data practices (Declarative M=3.67, SD=3.16) and low risk awareness (Cognitive M=3.56, SD=2.37), but very limited behavioral competence (Procedural M=0.68, SD=1.69). The composite DCPS score for each participant was calculated using the weighted sum product formula defined in the framework (DCPS Score = 0.3 * Declarative + 0.3 * Cognitive + 0.4 * Procedural). The overall mean DCPS score of all participants is 2.44 on a 0-10 scale with SD = 1.85, reflects a low overall level of AI privacy literacy in Generation Z.

Table VIII also shows that nearly 69% of respondents scored zero on the procedural subscale, indicating minimal engagement with privacy settings. In contrast, none scored zero on the cognitive subscale, indicating moderate level of risk awareness.

TABLE VIII. DESCRIPTIVE STATISTICS OF DCPS PRIVACY LITERACY FRAMEWORK (0-10 SCALE, N = 73)

| Knowledge | Mean | SD | % of zero knowledge | Interpretation |
|---|---|---|---|---|
| **Declarative** | 3.67 | 3.16 | 15% | Low level of factual knowledge |
| **Cognitive** | 3.56 | 2.37 | 0% | Low level of risk awareness |
| **Procedural** | 0.68 | 1.69 | 69% | Very low level of behavior competency |
| **DCPS Score** | 2.44 | 1.85 | — | Low overall score |

### D. Disscussions

*1) Declarative Knowledge of Privacy Literacy:* Six categories were represented by fourteen factual questions covering prompt/content data, device information, account data, profiling, data retention, and deletion policies. Items initially considered redundant (e.g., file and image uploads) were retained after response analysis showed distinct answer patterns. Future research should examine item intercorrelation to assess possible multicollinearity or redundancy, ensuring that highly correlated indicators do not inflate reliability coefficients or obscure meaningful subtopics within declarative knowledge.

As an indicator of declarative reliability, familiarity with the term "jailbreaking" was assessed. Only 20.5% of participants recognized the term, and of those, most accurately defined it as "bypassing AI safety restrictions." Students familiar with "jailbreaking" demonstrated slightly higher declarative scores, confirming that comprehension of AI terminology aligns with measured factual knowledge.

*2) Cognitve Knowledge of Privacy Literacy:* This dimension assessed evaluative reasoning about privacy risks, control, and trust using five items grouped into three conceptual variables: (a) risk awareness, (b) misconception recognition, and (c) perceived control. While the pilot employed a survey format, future studies could supplement these measures with qualitative reasoning tasks or semi-structured interviews to capture how users justify privacy decisions. Future research could further refine this subscale by expanding each conceptual variable into multiple balanced indicators, enabling broader coverage of cognitive reasoning in AI privacy contexts.

In the pilot study, Generation Z did not show strong overall privacy-risk sensitivity (M=3.56) on 0-10 scale. However, when asked directly whether pasting personal information could result in risk, the single-item score rose to 8-9, indicating relative risk awareness. When similar questions

were framed differently, perceived risk declined, suggesting that this variation may reflect not only sensitivity to item wording but also limited declarative understanding or misconceptions about data handling in Gen AI systems.

*3) Procedual Knowledge of Privacy Literacy:* Procedural competence, measured through awareness, actions, and perceived success in managing AI privacy settings, showed the lowest performance. Only 21 students (29%) reported visiting AI privacy settings at least once; four attempted changes (three partly successful and one fully successful). Thirty-nine (53%) had never accessed these settings, and 11 (15%) were unaware such options existed. Thus, 82% of respondents demonstrated minimal or nonexistent engagement with privacy controls, underscoring usability issues in how these settings are communicated and accessed. Because procedural competence reflects the behavioral translation of knowledge and awareness, these findings point to a critical gap in usability design and public education rather than user indifference alone. The absence of awareness and failure to complete privacy actions suggest that current AI platforms do not effectively support users in learning or managing their data protection.

*4) Summary:* The gap between awareness and action reflects the well-documented privacy paradox, users express concern but seldom act protectively. In the context of generative AI, this paradox highlights persistent challenges in translating risk awareness into effective privacy behavior.

Findings from this pilot study illustrates the conceptual structure of the DCPS privacy literacy framework and highlight a consistent gap between awareness and action in AI privacy literacy. Generation Z participants demonstrated low level of declarative literacy, reflecting strong risk awareness when right question being asked and evaluative judgment about privacy in generative-AI contexts. However, this awareness did not translate into behavioral competence: Procedural literacy was markedly low, with most participants reporting no engagement with privacy settings. This discrepancy reinforces the well-documented privacy paradox; individuals demonstrate privacy concern but fail to act protectively. The relative low level of Declarative literacy scores further suggest that while participants possess partial factual understanding of Gen AI data practices, this knowledge remains uneven and mixed with misconceptions. From a design perspective, results highlight the need for clearer interface communication of privacy settings and data-use explanations. From an educational perspective, the DCPS framework provides a structured tool for integrating privacy-literacy modules into digital-literacy curricula, supporting both classroom evaluation and curriculum design.

Overall, this pilot provides an initial baseline of Generation Z's AI privacy literacy using the DCPS framework. Results show that while participants recognize privacy risks and demonstrate some factual understanding, few translate that awareness into protective behavior. The observed gap between awareness and procedural action highlights where future educational and design efforts should focus. These descriptive findings illustrate how the DCPS framework can be applied to map different types of privacy competence and identify areas for further refinement.

## V. Conclusion, Implications, and Future Work

This study proposed the DCPS (Declarative Cognitive Procedural Score) framework to conceptualize and assess privacy literacy and applied it to the context of generative AI. While few established measures exist for evaluating users' privacy competence with large language models, the DCPS framework provides a structured foundation that can be adapted across platforms and populations. The pilot results show that declarative and cognitive understanding do not necessarily translate into procedural competence, a pattern consistent with the privacy paradox. The lack of awareness of privacy settings highlights a usability gap in how AI systems communicate privacy options, while low success in completing privacy actions suggests challenges in ease of learning and accessibility.

The DCPS privacy literacy framework, by providing both a baseline score and a measurement structure, offers a tool for future research to benchmark AI privacy literacy and to design targeted interventions for improving user understanding and action. Developing cost-effective, survey-based measures such as DCPS enables researchers and educators to systematically identify discrepancies between literacy and usability gaps and to guide both design improvements and privacy-education initiatives.

These findings confirm that privacy literacy is multidimensional and that declarative, cognitive, and procedural competencies must be measured separately to capture meaningful differences among users. The DCPS framework offers both a theoretical and methodological foundation for doing so. It differentiates knowing, reasoning, and doing, providing a comprehensive structure that future studies can adapt for different AI or platform contexts. The pilot also demonstrates the feasibility of a standardized 0 -10 privacy-literacy scoring system, enabling comparison across samples and educational interventions.

This pilot study was exploratory and limited by its small, single-institution Generation Z sample. Although the revised DCPS privacy literacy instrument improves conceptual alignment, further validation with larger and more diverse populations is needed. Both the Cognitive and Procedural subscales require further refinement to improve their measurement. Future research should refine the instrument, expand the item pool, and explore how usability design, educational efforts, and system transparency shape privacy literacy development.

The DCPS privacy literacy framework advances understanding of AI privacy literacy by integrating declarative, cognitive, and procedural knowledge dimensions into a unified model grounded in verifiable factual knowledge of generative AI data practices. Building on prior e-commerce privacy literacy research, its declarative component employs a Likert-scale factual-knowledge approach to reduce guessing and enhance measurement. The pilot study establishes an empirical baseline, showing that Generation Z users recognize privacy risks but lack the procedural skills needed to act effectively. The DCPS structure and its scoring system provide a replicable, adaptable, and cost-effective instrument for assessing and improving privacy literacy for generative AI.

## REFERENCES


[1] W. D. Heaven, "ChatGPT is everywhere. here's where it came from," *MIT Technology Review*. February 2023. [online]. Available: https://www.technologyreview.com/2023/02/08/1068068/chatgpt-is-everywhere-heres-where-it-came-from/

[2] B. Y. Ng, Li, J., Tong, X., Ye, K., Yenne, G., Chandrasekaran, V., and Li, J., "Analyzing security and privacy challenges in generative AI usage guidelines for higher education," 2025, arXiv:2506.20463 [online]. Available: https://arxiv.org/abs/2506.20463

[3] S. Trepte, Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., and Lind, F., "Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale," (OPLIS). In *Law, Governance and Technology Series*, pp. 333–365, Springer. 2014. [online]. Available: https://doi.org/10.1007/978-94-017-9385-8_14

[4] C. Prince, Omrani, N., Maalaoui, A., Dabic, M., and Kraus, S, "Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns," *IEEE Transactions on Engineering Management*, 70(10), pp. 3553–3570. 2023. [online]. Available: https://doi.org/10.1109/tem.2021.3092702

[5] Cisco. "New Cisco survey shows strong relationship between privacy awareness and trust in AI," Cisco Newsroom, October 2024. [online]. Available:https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m10/cisco-survey-shows-strong-relationship-between-privacy-awareness-and-trust-in-ai.html

[6] Y. Zhang, Wu, M., Tian, G. Y., Zhang, G., and Lu, J., "Ethics and privacy of artificial intelligence: Understandings from bibliometrics," *Knowledge-Based Systems*, 228. 2021. [online]. Available: https://doi.org/10.1016/j.knosys.2021.106994

[7] J. Hua, and Wang, P. "Cross-cultural privacy literacy in e-commerce: Testing users' understanding of platform data practices," *Issues in Information Systems*, 26(2), 323-334. 2025. [online]. Available: https://doi.org/10.48009/2_iis_125

[8] S. Choi, "Privacy literacy on social media: Its predictors and outcomes," *International Journal of Human–Computer Interaction*, 39(1), 217–232. 2022. [online]. Available: https://doi.org/10.1080/10447318.2022.2041892

[9] R. Ma and Chen, J. "Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior," *Frontiers in Psychology*, 14. 2023. [online]. Available: https://doi.org/10.3389/fpsyg.2023.1224168

[10] Y. J. Park, "Digital literacy and privacy behavior online," *Communication Research*, 40*(*2), 215 - 236. 2011. [online]. Available: https://doi.org/10.1177/0093650211418338

[11] C. K. Y. Chan and Hu, W. "Students' voices on generative AI: Perceptions, benefits, and challenges in higher education," *International Journal of Educational Technology in Higher Education*, 20(43). 2023. [online]. Available: https://doi.org/10.1186/s41239-023-00411-8

[12] J. Hua and Cunningham, J. "Two years after ChatGPT: A thematic analysis of first-year students' reflections on AI tool use in higher education," *Journal of Information, Communication and Ethics in Society*. 2025. [online]. Available: https://doi.org/10.1108/JICES-05-2025-0118

[13] A. Carolus, Koch, M., Straka, S., Latoschik, M. E., and Wienrich, C., "MAILS – Meta AI Literacy Scale: Development and testing of an AI literacy questionnaire based on well-founded competency models and psychological change- and meta-competencies," *ACM Transactions on Computer-Human Interaction*, 30(6), pp. 1-26. 2023. DOI: 10.1145/3593014.

[14] M. Mansoor, Pereira, D. G., and Syed, S. G.. "AI literacy among university students: A comparative transnational survey," *Frontiers in Communication*, 9(14), pp. 1–14, 2024, doi: 10.3389/fcomm.2024.1420032.

[15] B. Y. Ng, Li, J., Tong, X., Ye, K., Yenne, G., Chandrasekaran, V., and Li, J., "Design and validation of the AI Literacy Questionnaire: The Affective, Behavioural, Cognitive, and Ethical (ABCE) model," *Computers & Education*, 208, 2024. doi:10.1016/j.compedu.2024.108703.

[16] O. Rakhmanov, *A survey study on methods and techniques to measure online privacy knowledge* [Technical report]. ResearchGate. March 2021. [online]. Available: https://www.researchgate.net/publication/349724960

[17] J. Hua, *A comparative study of eCommerce data privacy between the U.S. and China.* (Doctoral dissertation, Robert Morris University). *ProQuest Dissertations Publishing*. 2025.