Open Access Library Journal
2026, Volume 13, e15305
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Factors Influencing Online Privacy Literacy in Generative AI Contexts: A Multidimensional Development Theory Perspective Based on Undergraduate Students in Zhejiang, China

Yuhan Xue, Luhao Wang, Yanqing Wang

School of Education, Zhejiang Normal University, Jinhua, China
Email: 2124329836@qq.com

How to cite this paper: Xue, Y.H., Wang, L.H. and Wang, Y.Q. (2026) Factors Influencing Online Privacy Literacy in Generative AI Contexts: A Multidimensional Development Theory Perspective Based on Undergraduate Students in Zhejiang, China. *Open Access Library Journal*, **13**: e15305.
https://doi.org/10.4236/oalib.1115305

Received: April 7, 2026
Accepted: May 23, 2026
Published: May 26, 2026

Abstract

With the rapid diffusion of generative artificial intelligence (Gen AI), its widespread use among undergraduate students has introduced new privacy challenges. Drawing on multidimensional development theory (MDT), this study examines the determinants of online privacy literacy in Gen AI contexts, using Internet Users' Information Privacy Concerns (IUIPC) as a proxy. Data from 224 undergraduate students in Zhejiang Province were analyzed using PLS-SEM. The results show that risk aversion, information sensitivity, perceived privacy protection measures, and social presence have significant positive effects on IUIPC, with risk aversion being the strongest predictor. In contrast, familiarity with government privacy regulations, prior privacy invasion experience, internet knowledge, and perceived benefits of information disclosure are not significant. These findings indicate that privacy concern formation in Gen AI environments is context-dependent and differs from traditional online settings. The study extends MDT to human–AI interaction contexts and provides implications for privacy education and platform design.

Subject Areas

Artificial Intelligence

Keywords

Multidimensional Development Theory, Online Privacy Literacy, Generative Artificial Intelligence, PLS-SEM, Privacy Concerns

1. Introduction

In recent years, Generative Artificial Intelligence (Gen AI) in China has developed rapidly. Domestic large language models such as Qwen and DeepSeek have been increasingly integrated into social life and are widely used by undergraduate students in learning, practice, and academic research, thereby reshaping patterns of knowledge production and learning. However, the widespread adoption of Gen AI has also raised growing concerns regarding privacy and security, which are particularly prominent among undergraduate populations. Due to their high acceptance and frequent use of Gen AI, undergraduate students face an elevated risk of privacy leakage.

Gen AI lacks explicit ethical norms and clearly defined privacy boundaries. Combined with its highly anthropomorphic interaction style, users may become less vigilant about privacy protection during use, leading to the unconscious disclosure of personal information. Therefore, examining the key factors influencing privacy concerns among undergraduate students in the context of Gen AI is essential for improving AI privacy governance, enhancing students' privacy awareness, and ensuring the healthy application of Gen AI in higher education settings.

Existing studies have mainly focused on online privacy concerns and information disclosure. From the perspective of privacy calculus, individuals' decisions are viewed as a trade-off between perceived benefits and risks, and the privacy paradox—the inconsistency between attitudes and behaviors—is widely observed. The Antecedents-Privacy Concerns-Outcomes framework further suggests that individual, contextual, and environmental factors jointly shape privacy concerns and related behaviors. However, most studies have concentrated on traditional social and e-commerce contexts, with limited attention to emerging human-AI conversational environments.

The anthropomorphic interaction and personalization features of Gen AI reshape users' perceptions and decision-making processes. Privacy disclosure is increasingly influenced by trust and immersion, while personalization may exacerbate users' privacy vulnerability and lead to context-dependent behavioral differences [1]. Nevertheless, the mechanisms underlying privacy concerns in Gen AI contexts remain insufficiently integrated and lack comprehensive empirical evidence.

Accordingly, this study focuses on undergraduate students from Zhejiang Province, China, to investigate the key factors and mechanisms influencing privacy concerns in Gen AI usage. Theoretically, it integrates the IUIPC framework, the privacy paradox, and multidimensional development theory to extend the explanatory power of privacy research in human-AI interaction contexts. Practically, it provides implications for privacy education in universities and for optimizing privacy design in Gen AI platforms, aiming to balance technological advancement and privacy protection.

2. Literature Review

2.1. Definition and Connotation of Online Privacy Literacy

Research on online privacy literacy can be traced back to Barnes' proposal of the

"Privacy Paradox", which refers to the inconsistency between individuals' privacy attitudes and their actual behaviors [2]. On this basis, scholars have gradually incorporated privacy literacy into the framework of digital literacy, considering it a core capability for individuals to understand, evaluate, and manage privacy information in digital environments [3]. Further studies have refined this concept from the perspective of knowledge structure, defining it as a combination of declarative knowledge (awareness of privacy risks and rules) and procedural knowledge (the ability to implement privacy protection behaviors) [4]. S. Trepte first introduced the concept of "Online Privacy Literacy", arguing that one of the reasons for the inconsistency between users' privacy protection behaviors and attitudes lies in the lack of knowledge and skills related to privacy tools [5]. Weinberger *et al.* further categorized online privacy literacy into two dimensions: passive privacy literacy and active privacy literacy [6]. Wissinger *et al.* emphasized that the definition of privacy literacy focuses on understanding the responsibilities and risks associated with sharing information online [7]. Deng Shengli *et al.* argued that online privacy literacy refers to users' mastery of knowledge and skills related to privacy protection [8].

2.2. Measurement of Online Privacy Literacy

In terms of measurement, existing studies have primarily drawn on classical models in information privacy research and have gradually developed multidimensional measurement instruments. Among them, the Concern for Information Privacy (CFIP) [9] and the Internet Users' Information Privacy Concerns (IUIPC) [10] models have been widely applied. The former conceptualizes consumers' privacy concerns from the perspective of organizational behavior, attributing them to worries about improper organizational practices in data collection, errors, secondary use, and unauthorized access. The latter, grounded in social contract theory, consists of three dimensions: collection, control, and awareness. In addition, with the advancement of privacy literacy research, scholars have begun to develop dedicated measurement scales that operationalize online privacy literacy across dimensions such as knowledge, skills, and behaviors. Some studies have further incorporated variables such as risk perception and privacy management ability to expand traditional measurement frameworks [3] [11]-[13].

2.3. Influencing Factors of Online Privacy Literacy

Regarding the influencing factors of online privacy literacy, existing studies have not yet formed a unified theoretical framework, but a trend toward multi-theoretical integration has emerged. On the one hand, research based on the Technology Acceptance Model and Protection Motivation Theory emphasizes psychological variables such as perceived usefulness, risk perception, and self-efficacy in influencing privacy behaviors; on the other hand, Social Cognitive Theory and multidimensional development theory explain the formation mechanism of privacy literacy from multiple perspectives, including individual experience, social environ-

ment, and informational context. Empirical studies generally find that internet usage experience and learning experience significantly promote privacy literacy [14] [15], while demographic variables (such as gender and age) show inconsistent effects across studies [12] [16] [17]. In addition, individual knowledge level, internet usage experience, socioeconomic status, motivational factors, benefit factors, and privacy concerns [8] are also influencing factors of online privacy literacy. Overall, although current studies have identified multiple influencing factors, most adopt a single-theory approach and lack a systematic integration of multidimensional interaction mechanisms.

2.4. Research Model

In summary, existing research on online privacy literacy has made certain progress in conceptual definition, measurement methods, and identification of influencing factors, but several limitations remain. First, at the theoretical level, most studies rely on a single perspective such as the Technology Acceptance Model or risk perception theory, lacking an integrated cross-theoretical framework, which makes it difficult to fully explain privacy decision-making mechanisms in complex contexts. Second, in terms of research perspective, related studies are mainly grounded in social psychology or communication paradigms, with insufficient interdisciplinary integration. Third, regarding research subjects, systematic studies focusing on undergraduate populations remain limited, failing to fully capture their emerging behavioral characteristics in generative artificial intelligence environments. Although some studies have attempted to integrate perspectives such as multidimensional development theory, they still remain largely within static analytical frameworks and lack in-depth exploration of the dynamic evolution mechanisms of privacy literacy and the interaction effects among multiple factors, which also constitutes the entry point of this study.

3. Research Design

3.1. Measurement of Online Privacy Literacy

As a multidimensional construct, online privacy literacy currently lacks a unified and well-established quantitative measurement instrument. Given that IUIPC can systematically capture individuals' cognition and concern regarding privacy issues from three dimensions—collection, control, and awareness—and has been widely applied in numerous privacy-related studies, this study adopts IUIPC as a proxy operationalization of online privacy literacy. This approach can, to a certain extent, reflect individuals' levels of concern and risk awareness when facing information disclosure situations, thereby providing a feasible measurement basis for analyzing the influence of multidimensional development factors on privacy cognition.

Following this perspective, the present study focuses on the cognition-centered dimension of online privacy literacy and operationalizes it through IUIPC in order to examine how multidimensional developmental factors shape privacy-re-

lated perceptions in generative AI usage.

3.2. Research Hypotheses

The multidimensional development theory (MDT) proposed by Laufer and Wolfe provides a comprehensive description of the multidimensional factors that influence individuals' privacy perceptions and privacy violations [18]. According to MDT, any privacy situation can be described from four dimensions: environmental, personal, information management, and interaction management. Compared with other theories primarily based on privacy calculus concepts (such as utility maximization theory), MDT enables a more comprehensive understanding of the antecedents of privacy concerns [19]. The research hypotheses of this study are presented in **Figure 1**.

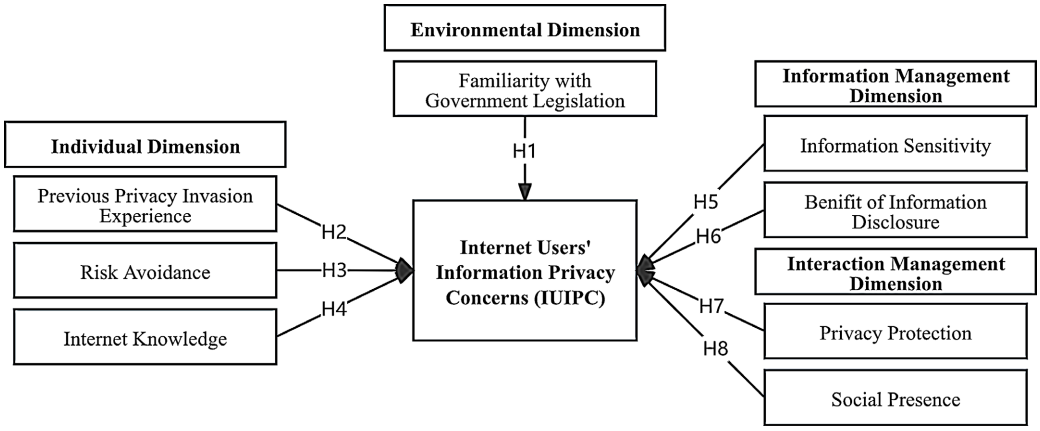

Figure 1. Research model.

1) Environmental Dimension

The environmental dimension refers to the elements that constitute the meaning of privacy and the boundaries of user experience, which play a critical role in shaping individuals' perceptions, access, and ability to use available privacy options. Government regulations, industry self-regulation, and cultural values have been identified as three major environmental factors influencing individuals' perceptions of online privacy literacy. In this study, industry and cultural values are not included as research variables and are therefore excluded. As an important institutional safeguard, government legislation can enhance individuals' trust in privacy protection and their level of awareness. Therefore, the higher an individual's familiarity with government legislation, the lower their level of privacy concerns.

H1: Familiarity with government legislation negatively affects individuals' IUIPC.

2) Individual Dimension

This dimension refers to the influence of individuals' developmental processes on their privacy perceptions. Privacy perceptions are shaped and formed by each individual in daily life based on their educational background, past experiences, and psychological characteristics [20]. The individual dimension includes three

categories: prior privacy invasion experiences, psychological and personality traits, and demographic variables. Among them, previous privacy invasion experience strengthen individuals' sensitivity to privacy risks; risk avoidance reflects individuals' conservative psychological tendencies; and internet knowledge level affects their ability to understand privacy-related issues, often leading to greater privacy concerns and awareness. Based on this, we propose:

H2: Previous privacy invasion experience positively affects IUIPC.

H3: Risk avoidance positively affects IUIPC.

H4: Internet knowledge positively affects IUIPC.

3) Information Management Dimension

Information management refers to the management of information disclosure through balancing benefits and risks, which largely reflects the concept of "privacy calculus" discussed earlier [21]. It refers to the inherent trade-off between the benefits obtained from disclosing personal information to a website and the risks of privacy loss resulting from such disclosure. We argue that higher information sensitivity leads to stronger individual concerns about privacy risks, while higher perceived benefits of information disclosure reflect greater cognitive complexity in privacy trade-offs:

H5: Information sensitivity positively affects IUIPC.

H6: Perceived benefit of information disclosure positively affects IUIPC.

4) Interaction Management Dimension

This dimension reflects efforts to optimize exchange mechanisms so that individuals have greater control over information exchange situations and better capabilities for balancing benefits and risks [22]. In online environments, interaction management can be achieved through direct approaches (e.g., providing privacy statements, privacy-enhancing technologies) or indirect approaches (e.g., improving website reputation). In this study context, well-developed privacy protection mechanisms can enhance individuals' perceived control over information, thereby reducing uncertainty and strengthening their concerns about privacy issues. At the same time, higher social presence can enhance users' sense of realism during interaction, making them more attentive to potential risks associated with personal information disclosure.

H7: Privacy protection positively affects IUIPC.

H8: Social presence positively affects IUIPC.

3.3. Methodology

This study adopts an empirical research method. Data are collected through a questionnaire survey, and Partial Least Squares Structural Equation Modeling (PLS-SEM) is employed to test the research hypotheses. PLS-SEM is suitable for analyzing models that include multiple latent variables and complex path relationships. It also imposes relatively low requirements on data distribution and can effectively handle small sample sizes or non-normal data, making it appropriate for testing the theoretical model in this study.

The measurement variables in this study include two categories: independent variables and dependent variables. All measurement scales are adapted from well-established studies in both domestic and international literature and are appropriately adjusted to fit the research context. A five-point Likert scale is used for measurement.

1) Dependent Variable

The dependent variable is Internet Users' Information Privacy Concerns (IUIPC), measured based on the scale developed by Malhotra *et al.* [10], covering three dimensions: Collection, Control, and Awareness. The specific measurement items are presented in Table 1.

Table 1. Measurement items adapted from IUIPC.

Dimension	Coding	Items
Collection	COL1	It usually bothers me when Gen AI websites ask me for personal information
	COL2	When Gen AI websites ask me for personal information, I sometimes think twice before providing it
	COL3	I am concerned that Gen AI websites are collecting too much personal information about me Internet
Control	CON1	It usually bothers me when I do not have control of the personal information that I provide to Gen AI websites
	CON2	It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by Gen AI websites
	CON3	I am concerned when control is lost or unwillingly reduced as a result of a marketing transaction with Gen AI websites
Awareness	AWA1	It usually bothers me when online privacy policy does not have a clear and conspicuous disclosure
	AWA2	It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by Gen AI websites
	AWA3	It usually bothers me when Gen AI websites seeking my information online do not disclose the way the data are collected, processed, and used

2) Independent Variables

Based on the MDT, this study classifies the influencing factors into four dimensions: environmental, individual, information management, and interaction management, which are operationalized into the following variables:

a) Environmental Dimension: Familiarity with Government Legislation (FAMLEG)

b) Individual Dimension: Previous Privacy Invasion Experience (PREEXP), Risk Avoidance (RISK), and Internet Knowledge (KNOW)

c) Information Management Dimension: Information Sensitivity (INFSEN) and Benefit of Information Disclosure (INFBEN)

d) Interaction Management Dimension: Privacy Protection (PORT) and Social Presence (SOC)

The measurement scales are adapted from the study by Hong *et al.* [19], and the specific items are presented in Table 2.

Table 2. Measurement Items for MDT.

Aggregate Dimensions	Secondary Dimensions	Coding	Items
Environmental Dimension	Familiarity with Government Legislation	FAMLEG1	I am fully aware that the Chinese government has a Privacy Policy to protect my privacy
		FAMLEG2	I am familiar with the Privacy Policy issued by the Chinese government
Individual Dimension	Previous Privacy Invasion Experience	PREEXP1	How often have you personally experienced incidents whereby your personal information was used by some Gen AI websites without your authorization?
		PREEXP2	How often have you personally been the victim of what you felt was an improper invasion of privacy by Gen AI websites?
	Risk Avoidance	RISK1	I would rather be safe than sorry
		RISK2	I am cautious in trying new or different things
		RISK3	I avoid risky things
	Internet Knowledge	KNOW1	I am knowledgeable about the Internet and its related privacy issues
		KNOW2	I am knowledgeable about latest developments that address Internet privacy issues
Information Management Dimension	Information Sensitivity	INFSEN1	When I am required to provide personal information to websites in exchange of their services, the information that they ask for are usually very sensitive personal information
		INFSEN2	Gen AI websites tend to ask me for sensitive personal information in order to obtain their services
	Benefit of Information Disclosure	INFBEN1	The benefits that I can obtain by providing my personal information to Gen AI websites are usually significant
		INFBEN2	I value the benefits that I can obtain by providing my personal information to Gen AI websites
Interaction Management Dimension	Privacy Protection	PORT1	In general, websites would ask for my authorization before collecting my personal information
		PORT2	In general, Gen AI websites would use privacy protection tools
		PORT3	In general, Gen AI websites would include a privacy policy statement on their websites
		PORT4	In general, Gen AI websites would let me aware the purpose of collecting my personal information
	Social Presence	SOC1	There is a sense of human contact in Gen AI websites
		SOC2	There is a sense of personalness in Gen AI websites
		SOC3	There is a sense of human warmth (or sensitivity) in Gen AI websites

3.4. Data Source and Sample Characteristics

This study collected data through an online questionnaire platform, targeting undergraduate students in Zhejiang Province who have experience using Gen AI. Prior to the formal survey, a pilot test with 20 respondents was conducted to en-

sure the clarity and comprehensibility of the measurement items. A total of 250 questionnaires were collected in the formal survey. To ensure data quality, responses were excluded if they were completed in an unreasonably short time, contained substantial missing values, or exhibited highly repetitive answer patterns, which are widely recognized indicators of invalid survey responses. After excluding invalid responses, 224 valid samples were obtained, yielding an effective response rate of 89.6%.

Among the 224 undergraduate respondents, 99 were male, accounting for 44.2% of the valid sample, and 125 were female, accounting for 55.8%, indicating a relatively balanced gender distribution.

In terms of grade level, respondents were mainly concentrated in the second year (39.3%) and third year (26.3%), followed by first-year students (24.1%), with fewer participants from other grades.

Regarding academic majors, students in Social Sciences accounted for the largest proportion (44.64%), followed by Engineering and Applied Sciences (33.48%), while Humanities (15.18%) and Natural Sciences (6.70%) accounted for smaller proportions. The sample covers 12 major disciplinary categories in Chinese higher education, indicating a certain degree of disciplinary diversity and enabling a relatively comprehensive reflection of students' use of generative artificial intelligence and their privacy perceptions across different academic backgrounds.

4. Data Analysis

4.1. Descriptive Statistics

The study analyzed undergraduate respondents' usage of Gen AI. The results show that all respondents have experience using Gen AI, among which 37.3% use it daily and 36.9% use it 3 - 5 days per week, indicating that most students have developed relatively frequent usage habits. In terms of usage purposes, respondents mainly apply Gen AI to learning assistance (96.4%), academic writing support (83.1%), information search (69.8%), and improving work efficiency (62.2%), reflecting its widespread application in academic and information acquisition contexts. In addition, the duration of Gen AI use is mainly concentrated within 1 - 3 years (73.7%), which is generally consistent with the timeline of large-scale adoption of generative AI technologies. In contrast, regarding willingness to disclose personal information, respondents overall exhibit a moderately cautious attitude. The proportions of high willingness (6.3%) and low willingness (6.7%) are both relatively small, with most responses concentrated at a moderate level, indicating that users maintain a certain level of privacy awareness while remaining open to moderate information disclosure in specific contexts.

Descriptive statistical analysis of the IUIPC scale and its dimensions are shown in Table 3, we can see that the mean values for Collection, Control, and Awareness are 3.670, 3.488, and 3.513, respectively, with an overall mean of 3.557, indicating that respondents' overall level of privacy concern is moderately high. Among them, the Collection Dimension has the highest score, suggesting that respond-

ents are more concerned about excessive collection of personal information. The standard deviations are all around 0.8, indicating a moderate level of data dispersion. The skewness values are all negative (ranging from −1.22 to −0.786), indicating that respondents tend toward higher levels of privacy concern. The kurtosis values are all positive, suggesting that the data distribution is relatively concentrated with a slightly peaked characteristic. Overall, the data distribution is relatively stable and approximately follows a normal distribution, providing a solid basis for further structural analysis.

Table 3. Descriptive statistics of IUIPC dimensions.

	Collection	Control	Awareness	IUIPC
Mean	3.670	3.488	3.513	3.557
SD	0.882	0.875	0.901	0.781
Skewness	−1.03	−0.786	−1.044	−1.22
SE (Skewness)	0.163	0.163	0.163	0.163
Kurtosis	1.305	0.656	1.154	2.113
SE (Kurtosis)	0.324	0.324	0.324	0.324

4.2. Model Measurement Evaluation

1) Reliability Assessment of the Measurement Model

In this study, the reliability of the measurement scales was evaluated through internal consistency tests of the measurement items. Internal consistency was assessed using Composite Reliability (CR) and Cronbach's Alpha. For exploratory research, a CR value above 0.7 and a Cronbach's Alpha coefficient above 0.6 are considered acceptable. As shown in Table 4, all latent variables meet the required thresholds for both Composite Reliability and Cronbach's Alpha, indicating that the measurement model demonstrates good reliability.

Table 4. Reliability and validity assessment of the measurement model.

Latent Variable	Cronbach's Alpha	CR	AVE	Factor Loading	t-test	Dependent Variable
FAMLEG	0.823	0.916	0.845	0.948	19.434	FAMLEG1
				0.89	9.777	FAMLEG2
PREEXP	0.842	0.924	0.859	0.895	21.316	PREEXP1
				0.957	23.689	PREEXP2
RISK	0.917	0.947	0.857	0.941	123.835	RISK1
				0.966	168.204	RISK2
				0.867	29.905	RISK3
KNOW	0.728	0.871	0.772	0.949	59.338	KNOW1
				0.802	12.706	KNOW2

Continued

INFSEN	0.84	0.924	0.86	0.949	109.996	INFSEN1
				0.905	37.408	INFSEN2
INFBEN	0.802	0.91	0.835	0.909	9.04	INFBEN1
				0.919	12.638	INFBEN2
PORT	0.783	0.864	0.62	0.869	15.882	PORT1
				0.862	28.436	PORT2
				0.825	16.722	PORT3
				0.55	6.23	PORT4
SOC	0.786	0.859	0.674	0.66	3.403	SOC1
				0.928	6.308	SOC2
				0.851	5.641	SOC3
Collection	0.822	0.894	0.739	0.878	31.872	COL1
				0.883	39.898	COL2
				0.815	26.671	COL3
Control	0.921	0.95	0.864	0.919	67.789	CON1
				0.957	125.962	CON2
				0.912	55.372	CON3
Awareness	0.943	0.963	0.898	0.941	96.178	AWA1
				0.961	121.438	AWA2
				0.941	82.555	AWA3
IUIPC	0.857	0.913	0.778	0.89	46.027	Collection
				0.861	23.05	Control
				0.894	47.047	Awareness

2) Validity Assessment of the Measurement Model

Generally, factor loading greater than 0.5 are considered sufficient to reasonably explain the latent variables. As shown in **Table 5**, all factor loadings in this study meet the requirements for structural validity. In addition, convergent validity and discriminant validity in the PLS model are mainly assessed using the Average Variance Extracted (AVE). The AVE should exceed 0.5, and the square root of AVE should be greater than the correlations between the latent variable and other constructs [23]. The results indicate that the data satisfy these criteria, suggesting that the observed variables exhibit a strong linear correspondence with the latent variables and adequately explain them.

3) Evaluation of Model Predictive Power

The predictive power of the model is assessed using the coefficient of determination (R^2) of the endogenous constructs. A higher R^2 value indicates stronger explanatory power of the independent variables on the dependent variables. In

Table 5. Discriminant validity (Fornell–Larcker Criterion).

	FAMLEG	PREEXP	RISK	KNOW	INFSEN	INFBEN	PORT	SOC	IUIPC
FAMLEG	0.919								
PREEXP	−0.219	0.927							
RISK	0.345	0.206	0.926						
KNOW	0.596	0.171	0.448	0.879					
INFSEN	−0.099	0.763	0.162	0.172	0.927				
INFBEN	−0.157	0.646	−0.039	0.154	0.56	0.914			
PORT	0.335	0.264	0.4	0.365	0.271	0.272	0.788		
SOC	0.185	−0.155	0.009	0.184	−0.083	−0.083	−0.188	0.821	
IUIPC	0.244	0.354	0.547	0.411	0.399	0.251	0.45	0.168	0.882

this study, the significance of path coefficients was tested using the Bootstrap method with 1000 resamples. The model explains 49.3% of the variance in IUIPC ($R^2 = 0.493$), indicating a moderate level of explanatory power.

Furthermore, the results of the second-order construct IUIPC show that it is composed of three dimensions: Collection, Control, and Awareness. All paths are statistically significant ($p < 0.001$), indicating that the second-order structural model demonstrates good construct validity. Overall, the measurement quality and structural relationships in the model meet the requirements of PLS-SEM analysis, demonstrating satisfactory explanatory power and robustness.

4.3. Structural Model Explanation

Regarding the path relationships, as shown in Table 6 and Figure 2, Risk Avoidance ($\beta = 0.391$, $t = 4.16 > 1.96$), Information Sensitivity ($\beta = 0.228$, $t = 2.62 > 1.96$), Privacy Protection ($\beta = 0.231$, $t = 3.30 > 1.96$), and Social Presence ($\beta = 0.225$, $t = 3.63 > 1.96$) all have significant positive effects on IUIPC. Among these factors, Risk Avoidance exhibits the strongest effect.

Table 6. Hypothesis testing results.

Hypothesis	Path	β	Bootstrap SD	t-value	Result
H1	FAMLEG → IUIPC	−0.011	0.079	−0.14	Rejected
H2	PREEXP → IUIPC	0.012	0.085	0.14	Rejected
H3	RISK → IUIPC	0.391	0.094	4.16	Accepted
H4	KNOW → IUIPC	0.064	0.078	0.82	Rejected
H5	INFSEN → IUIPC	0.228	0.087	2.62	Accepted
H6	INFBEN → IUIPC	0.074	0.076	0.97	Rejected
H7	PORT → IUIPC	0.231	0.07	3.3	Accepted
H8	SOC → IUIPC	0.225	0.062	3.63	Accepted

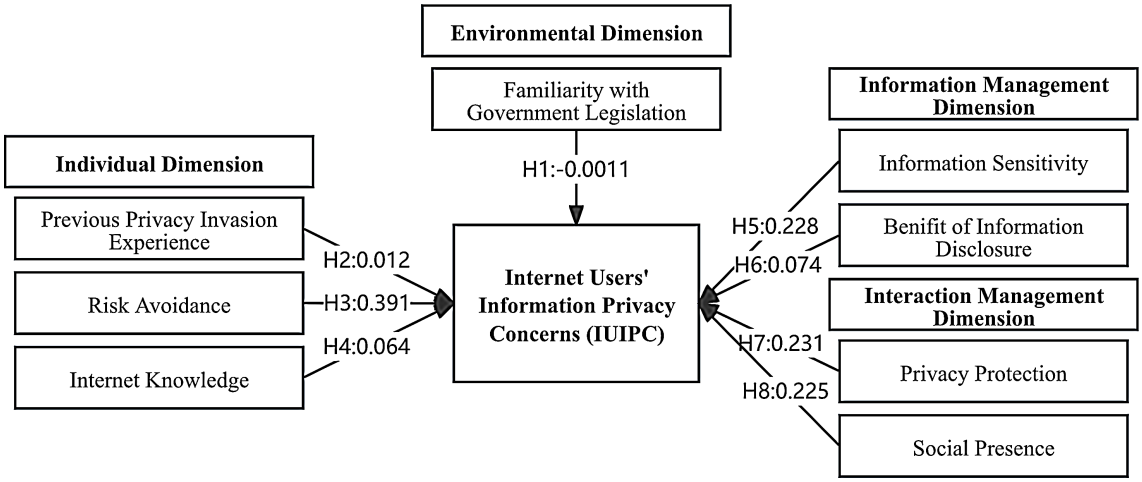

Figure 2. Hypotheses testing.

In contrast, Familiarity with Government Legislation, Previous Privacy Invasion Experience, Internet Knowledge, and Benefit of Information Disclosure do not show statistically significant effects on IUIPC.

5. Discussion

5.1. Core Characteristics of the Hypothesis Testing Results

This study constructs a model of factors influencing online privacy literacy among undergraduate students in the context of Gen AI based on the MDT and empirically tests it using PLS-SEM. These findings highlight the differences in privacy cognition mechanisms between Gen AI–mediated human–computer interaction contexts and traditional online environments.

Further analysis shows that the overall level of IUIPC among undergraduate students is moderately high, with the strongest concern observed in the dimension of Information Collection. Meanwhile, their willingness to disclose personal information exhibits a moderately cautious tendency. In terms of usage behavior, all respondents have experience using Gen AI, and more than 70% report usage frequencies of at least three days per week, primarily for academic purposes such as learning assistance and academic writing. This indicates that Gen AI has become deeply embedded in undergraduate students' learning and daily lives, and privacy concerns have evolved into a practical issue.

However, although undergraduate students possess a basic awareness of privacy protection, their privacy cognition systems have not yet fully adapted to the characteristics of Gen AI technologies. In this context, some traditional determinants of privacy concerns in conventional online environments appear to weaken or even lose their explanatory power in Gen AI settings.

5.2. Mechanisms of Influencing Factors across Dimensions

Within the Individual Dimension, Risk Avoidance emerges as the core factor influencing undergraduate students' privacy concerns (β = 0.391), which is con-

sistent with Social Cognitive Theory emphasizing the role of individual psychological traits in shaping privacy-related decision-making. As frequent users of generative artificial intelligence (Gen AI), undergraduate students possess a certain level of digital competence; however, when faced with ambiguous privacy boundaries and the irreversibility of information disclosure in Gen AI contexts, their risk-averse tendencies significantly amplify concerns regarding information collection, control, and awareness. In contrast, Previous Privacy invasion Experience and Internet Knowledge do not exhibits significant effects. This may be because such experiences are primarily rooted in traditional social networking and e-commerce contexts and have limited relevance to the novel privacy risks associated with Gen AI, thus hindering cross-contextual risk perception transfer. Meanwhile, internet knowledge among students tends to focus on basic operational skills, lacking domain-specific privacy knowledge related to Gen AI, and therefore cannot be effectively translated into privacy risk assessment capabilities.

With respect to the Information Management and Interaction Management Dimensions, the findings reveal distinct contextual characteristics of Gen AI environments. In the Information Management Dimension, only Information Sensitivity has a significant positive effect on IUIPC, whereas Benefits of Information Disclosure are not significant. This result partially supports the applicability of Privacy Calculus Theory while also highlighting its contextual limitations. Specifically, students adjust their privacy concerns based on the sensitivity of the information, with the disclosure of sensitive content—such as academic ideas and personal opinions—significantly increasing perceived risk. However, the benefits derived from Gen AI usage are primarily intangible, such as improved learning efficiency, which are often ambiguous and difficult to quantify. As a result, they cannot form a clear trade-off with privacy risks, thereby weakening the explanatory power of traditional privacy calculus mechanisms.

In the Interaction Management Dimension, both hypotheses are supported. Notably, the significant positive effect of Privacy Protection measures on IUIPC contrasts with prior research findings. This may be attributed to the complexity of Gen AI technologies, which leads students to interpret privacy policies and permission settings more as "risk cues" rather than "security assurances," thereby enhancing their awareness of potential risks. At the same time, the significant effect of social presence stems from the anthropomorphic interaction characteristics of Gen AI. A higher level of social presence enhances users' sense of realistic interaction, prompting them to transfer offline privacy perceptions into online human–AI interactions, which in turn increases their overall level of privacy concern.

Within the Environmental Dimension, Familiarity with Government Legislation does not show a significant effect, reflecting the limited dissemination and practical effectiveness of privacy regulations among university students. Students' understanding of privacy regulations tends to remain at a superficial level and has not developed into institutional trust regarding Gen AI-related privacy risks. Con-

sequently, regulatory awareness fails to establish stable expectations of privacy protection and does not effectively reduce privacy concerns.

In addition, the model explains 49.3% of the variance in IUIPC ($R^2 = 0.493$), indicating a moderate level of explanatory power. This suggests that factors not included in the model—such as privacy education in higher education, platform ethical governance, and peer influence—may also play important roles in shaping undergraduate students' online privacy literacy, and future research should further extend the analytical framework.

6. Conclusions

6.1. Key Findings

First, Gen AI has been deeply integrated into undergraduate students' academic and daily activities, with frequent usage primarily concentrated in learning assistance and academic writing. The overall level of privacy concern is moderately high, with the strongest concern observed in information collection. Students exhibit a moderately cautious attitude toward privacy disclosure, suggesting a potential inconsistency between privacy attitudes and behaviors, and highlighting the urgency of addressing privacy risks.

Second, within the MDT framework, only four factors—Risk Avoidance, Information Sensitivity, Privacy Protection, and Social Presence—have significant positive effects on IUIPC. Among these, Risk Avoidance exerts the strongest influence. These factors jointly shape privacy concerns from the perspectives of individual psychology, information cognition, platform mechanisms, and interaction experience.

Third, several key determinants of privacy concerns in traditional online contexts do not show significant effects in Gen AI environments. Familiarity with Government Legislation, Previous Privacy Invasion Experience, Internet Knowledge, and Benefits of Information Disclosure are all insignificant, indicating the context-specific nature of privacy concern formation in Gen AI settings and a mismatch between students' privacy cognition and technological development.

Fourth, the technological attributes and interaction features of Gen AI play a critical role in reshaping privacy concern mechanisms. Anthropomorphic interaction enhances social presence, while platform privacy protection mechanisms increase risk perception. Together, these factors disrupt traditional privacy cognition patterns and emerge as key drivers of privacy concerns in Gen AI contexts.

6.2. Limitations and Future Research

Despite its contributions, this study has several limitations. First, the sample is limited to undergraduate students in Zhejiang Province, which may restrict the universality of the findings. Second, IUIPC is used as a proxy for online privacy literacy, which captures privacy concerns but does not fully reflect its multidimensional nature, including knowledge, skills, and behaviors. Third, the use of cross-sectional data limits the ability to examine the dynamic evolution of privacy literacy.

Future research can be extended in several directions. First, expanding the sample to include diverse regions, educational levels, and occupational groups would improve the universality of the model. Second, developing context-specific, multidimensional measurement scales for online privacy literacy in Gen AI environments would enhance measurement accuracy. Third, adopting longitudinal research designs would enable the examination of the dynamic evolution of privacy literacy over time, while incorporating factors such as privacy education, platform governance, and social influence to further improve the explanatory power of the model.

Funding

Provincial Undergraduate Training Program on Innovation and Entrepreneurship (Number: S202510345026).

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Jiang, Y. and Duan, X. (2026) The Privacy Paradox and Algorithmic Resistance: Do Users Really Care about the Tailored Responses in Generative Artificial Intelligence. *International Journal of Human-Computer Interaction*, 1-25. https://doi.org/10.1080/10447318.2026.2631679

[2] Barnes, S.B. (2016) A Privacy Paradox: Social Networking in the United States. *First Monday*, **11**, 5-16.

[3] Rotman, D. (2005) Are You Looking at Me?—Social Media and Privacy Literacy. https://hdl.handle.net/2142/15339

[4] Bajnaid, W. and Aljasir, S. (2025) Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region. *Journalism and Media*, **6**, Article 8. https://doi.org/10.3390/journalmedia6010008

[5] Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A., *et al.* (2015) Do People Know about Privacy and Data Protection Strategies? Towards the "online Privacy Literacy Scale" (OPLIS). In: Gutwirth, S., Leenes, R. and de Hert, P. Eds., *Law, Governance and Technology Series*, Springer, 333-365. https://doi.org/10.1007/978-94-017-9385-8_14

[6] Weinberger, M., Zhitomirsky-Geffet, M. and Bouhnik, D. (2017) Factors Affecting Users' Online Privacy Literacy among Students in Israel. *Online Information Review*, **41**, 655-671. https://doi.org/10.1108/oir-05-2016-0127

[7] Wissinger, C. (2017) Privacy Literacy: From Theory to Practice. *Communications in Information Literacy*, **11**, 378-389. https://doi.org/10.15760/comminfolit.2017.11.2.9

[8] Deng, S., and Wang, Z. (2018) Review of Privacy Literacy Research Abroad. *Digital Library Forum*, **9**, 66-72.

[9] Smith, H.J., Milberg, S.J. and Burke, S.J. (1996) Information Privacy: Measuring Individuals' Concerns about Organizational Practices1. *MIS Quarterly*, **20**, 167-196. https://doi.org/10.2307/249477

[10] Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004) Internet Users' Information Privacy

Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, **15**, 336-355. https://doi.org/10.1287/isre.1040.0032

[11] Veghes, C., Orzan, M. and Acatrinei, C. (2012) Privacy Literacy: What Is and How It Can Be Measured? *Annales Universitatis Apulensis Series Oeconomica*, **2**, 704-711. https://doi.org/10.29302/oeconomica.2012.14.2.36

[12] Park, Y.J. (2013) Digital Literacy and Privacy Behavior Online. *Communication Research*, **40**, 215-236.

[13] Morrison, B. (2012) Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy. *Proceedings of the* 42*nd Atlantic Schools of Business conference*, Nova Scotia, 28 September 2012, 419-438.

[14] Bartsch, M. and Dienlin, T. (2016) Control Your Facebook: An Analysis of Online Privacy Literacy. *Computers in Human Behavior*, **56**, 147-154. https://doi.org/10.1016/j.chb.2015.11.022

[15] Bernadas, J.M.A.C. and Soriano, C.R. (2019) Online Privacy Behavior among Youth in the Global South: A Closer Look at Diversity of Connectivity and Information Literacy. *Journal of Information*, *Communication and Ethics in Society*, **17**, 17-30. https://doi.org/10.1108/jices-03-2018-0025

[16] Weinberger, M., Zhitomirsky-Geffet, M. and Bouhnik, D. (2017) Sex Differences in Attitudes towards Online Privacy and Anonymity among Israeli Students with Different Technical Backgrounds. *Information Research*. **22**, Article 777.

[17] Kezer, M., Sevi, B., Cemalcilar, Z. and Baruh, L. (2016) Age Differences in Privacy Attitudes, Literacy and Privacy Management on Facebook. *Cyberpsychology*: *Journal of Psychosocial Research on Cyberspace*, **10**, Article 2. https://doi.org/10.5817/cp2016-1-2

[18] Laufer, R.S. and Wolfe, M. (1977) Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, **33**, 22-42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

[19] Hong, W., Chan, F.K.Y. and Thong, J.Y.L. (2021) Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics*, **168**, 539-564. https://doi.org/10.1007/s10551-019-04237-1

[20] Westin, A.F. (2003) Social and Political Dimensions of Privacy. *Journal of Social Issues*, **59**, 431-453. https://doi.org/10.1111/1540-4560.00072

[21] Dinev, T. and Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, **17**, 61-80. https://doi.org/10.1287/isre.1060.0080

[22] Milne, G.R. (2000) Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing*, **19**, 1-6. https://doi.org/10.1509/jppm.19.1.1.16934

[23] Fornell, C. and Larcker, D.F. (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, **18**, 39-50. https://doi.org/10.1177/002224378101800104