Article

Disclosure Intention in Generative AI: Effects of Privacy Concern, Personalization Benefit, and Trust

Yinong Qiu , Pingjiayi Du, Jiaqi Zhang, Xiangkui Ding*

Kangwon National University, Chuncheon, 24341, Republic of Korea
*Correspondence: dingxiangkui@126.com

Citation: Qiu, Y. N., Du, P. J. Y., Zhang, J. Q., & Ding, X. K. (2025). Disclosure Intention in Generative AI : Effects of Privacy Concern, Personalization Benefit, and Trust. *Journal of Arts and Cultural Studies*, 4 (2), 1-16. https://doi.org/10.23112/acs25123001

Check for updates

Received: October 13, 2025
Revised: November 28, 2025
Accepted: December 19, 2025
Published: December 30, 2025

Abstract: ***Background:*** Generative AI enhances the efficiency of personalized services, but it also creates complex choices for users about what information to disclose during multi-turn interactions. Although prior research has examined privacy-related risk, personalization-related benefits, and trust, empirical evidence on their combined effects in generative AI contexts remains limited. ***Objective:*** Utilizing privacy calculus theory and incorporating a trust perspective, this study investigates how Privacy Concern, Perceived Personalization Benefit, and Trust affect Disclosure Intention in generative AI contexts and compares their relative explanatory power. ***Methods:*** Questionnaire data from 302 valid respondents were analyzed using reliability analysis, exploratory factor analysis, correlation analysis, and multiple linear regression. ***Results:*** Privacy Concern had a significant negative effect on Disclosure Intention, whereas Perceived Personalization Benefit and Trust had significant positive effects. Among the three predictors, Trust showed the strongest explanatory power, followed by Privacy Concern, while Perceived Personalization Benefit exhibited a comparatively weaker effect. ***Conclusion:*** Disclosure in generative AI contexts is not merely a simple cost-benefit analysis; rather, it reflects the combined influence of risk perception, expected benefits, and the assurance of relationships. This study extends the scope of disclosure research to include generative AI settings and offers practical implications for privacy governance, personalization design, and trust building.

Keywords: Generative AI; Personal information disclosure intention; Privacy concern; Perceived personalization benefit; Tust

1. Introduction

With the rapid advancement of generative AI technology, intelligent dialogue systems powered by large language models are rapidly expanding into scenarios including education, office work, search, content creation, consulting, and lifestyle services. Unlike traditional information systems, generative AI not only processes natural-language input but also generates personalized, context-aware responses through continuous interaction. This significantly enhances information retrieval efficiency and user experience. However, creating high-quality outputs from generative AI often requires users to continuously provide personal preferences, behavioral patterns, life experiences, and even sensitive information such as identity, health, financial status, and employment details across multiple rounds of dialogue. This means that while generative AI creates personalized value, it also places users in complex decision-making situations regarding personal information disclosure. On one hand, users seek more precise and useful services by sharing additional information; on the other hand, they may have concerns about the collection, storage, misuse, or leakage of their personal data. Consequently, the willingness of users to disclose personal information in generative AI contexts has become a critical issue for understanding human-computer interaction (HCI), platform governance, and the adoption of intelligent services (Acquisti et al., 2015; Belanger & Crossler, 2011; Leschanowsky et al., 2024; Papneja & Yadav, 2025).

Current research on personal information disclosure primarily focuses on scenarios such as social media, e-commerce, online platforms, and traditional intelligent systems. These discussions often center on variables like privacy calculus, perceived risks, personalized benefits, and technological trust (Dinev & Hart, 2006; Dienlin & Metzger, 2016; Smith et al., 2011; Yun et al., 2019). However, the application of these conclusions to generative AI contexts remains limited.

Firstly, information disclosure is not a one-time, static authorization but rather occurs through continuous input, contextual embedding, and dynamic adjustments during multi-round dialogues. This makes the disclosure process more interactive, continuous, and uncertain (Choi et al., 2025; Papneja & Yadav, 2025). Compared to the relatively clear information-collection points on traditional platforms, disclosure behavior in generative AI is often embedded within task interactions. This leads to more complex user judgments regarding information boundaries, intended uses, and potential consequences (Leschanowsky et al., 2024; Chakraborty et al., 2025).

Secondly, existing research often emphasizes either privacy risks, personalized benefits, or trust as standalone factors, rarely integrating all three into a unified analytical framework. This approach remains insufficient for systematically explaining the decision-making logic behind user disclosure in generative AI contexts (Fernandes & Pereira, 2021; Lappeman et al., 2023; Liu & Tao, 2022; Eitiveni et al., 2023). Furthermore, there is a lack of direct and clear empirical evidence on the directional impacts and relative explanatory power of privacy concerns, perceived personalized benefits, and trust on users' willingness to disclose personal information in generative AI settings (Choi et al., 2025; Papneja & Yadav, 2025). These findings highlight the theoretical necessity and practical value of re-examining the mechanisms behind personal information disclosure in generative AI scenarios.

Building on this foundation, this study examines personal information disclosure, privacy concerns, perceived personalized benefits, and trust, which collectively influence users' willingness to disclose information. Specifically, we investigate the directional impacts of these three variables and compare their relative explanatory power. To achieve this, we use empirical methods—including reliability testing, exploratory factor analysis, correlation, and regression analyses, using valid samples obtained from questionnaire surveys. These methods assess the factors that influence willingness to disclose in generative AI scenarios, revealing how users balance risk perception, benefit expectations, and relationship evaluations when deciding whether to share information.

The research contributions of this paper are reflected in several aspects. First, by situating personal information disclosure within the emerging intelligent-interaction scenario of generative AI, this study expands the technical application boundaries of existing research on disclosure. It addresses the practical needs of user data behavior studies amid the rapid growth of generative AI (Papneja & Yadav, 2025; Choi et al., 2025). Second, by integrating privacy concerns, perceived personalized benefits, and trust into a unified analytical framework across three dimensions, like risk mitigation, benefit motivation, and relationship assurance, it provides a more comprehensive explanation for the logic behind users' disclosure willingness in generative AI contexts (Dinev & Hart, 2006; Fernandes & Pereira, 2021; Eitiveni et al., 2023). Third, while examining the significant impacts of various antecedent variables on disclosure willingness, this study further compares their relative explanatory power, offering multi-layered empirical evidence to clarify user decision-making mechanisms in generative AI scenarios. Fourth, the findings of this study offer practical insights for generative AI platforms in designing privacy protection mechanisms, presenting personalized value, and building user trust. These insights can help platforms enhance service efficiency while better balancing data utilization and privacy governance (Aguirre et al., 2015; Aguirre et al., 2016; Tucker, 2014; Liu & Sun, 2024).

Based on the above analysis, this paper proposes the following core research questions:

RQ1: In generative AI applications, do privacy concerns, perceived personalized benefits, and trust significantly influence users' willingness to disclose personal information? What are the specific directions of these impacts?

RQ2: Among privacy concerns, perceived benefits of personalization, and trust, which factor has the strongest explanatory power for users' willingness to disclose personal information?

2. Theoretical Basis and Literature Review

Personal information disclosure involves a decision-making process under conditions of uncertainty. Existing research generally suggests that individuals do not simply accept or reject disclosure; instead, they carefully evaluate potential risks, expected benefits, and assurances from their relationships (Phelps et al., 2000; Dinev & Hart, 2006; Smith et al., 2011). Based on this idea, the present study adopts privacy calculus theory as its primary explanatory framework. This theory suggests that individuals simultaneously assess the anticipated costs and benefits of disclosing personal information. When perceived costs are higher than expected benefits, willingness decreases; when expected benefits are greater, willingness increases (Dinev & Hart, 2006; Dienlin & Metzger, 2016; Fernandes & Pereira, 2021; Eitiveni et al., 2023). In generative AI contexts, "Privacy Concern" refers to users' perceptions of losing control over their information, as well as fear of misuse and data leakage. On the other hand, "Perceived Personalization Benefit" represents their expectations that disclosure will lead to more accurate, relevant, and high-quality services. However, the way generative AI operates is often complex and not transparent, making it difficult for users to fully understand how their inputs are processed, stored, and used. The present study incorporates a trust perspective to explain how users can reduce their psychological defensiveness and form more proactive decisions about sharing their information in uncertain technological environments (Gefen et al., 2003; Gefen et al., 2008; Pavlou, 2003; Ding & Zhou, 2025). On this basis, the study focuses on three core factors—Privacy Concern, Perceived Personalization Benefit, and Trust—to systematically examine their effects on Disclosure Intention in generative AI contexts.

2.1 Privacy Concern and Disclosure Intention

Privacy Concern refers to individuals' subjective fear that they may lose control over their personal information during its collection, storage, processing, sharing, and use, thereby facing risks such as leakage, misuse, or unauthorized expansion of use. In this context of digital technology, such concern reflects not only direct worries about information security but also users' sensitivity to a platform's data governance practices, usage boundaries, and accountability mechanisms (Malhotra et al., 2004; Smith et al., 2011; Bélanger & Crossler, 2011). Compared with traditional platforms, which typically use static and one-time authorization settings, personal information disclosure in generative AI is more continuous, contextualized, and interaction-embedded. Users often provide additional background information, preferences, and even personal experiences across multiple conversational exchanges to receive more contextually appropriate responses. Although this interaction pattern improves service adaptability, it also blurs the line between routine input and significant personal disclosure, thereby intensifying users' perceptions of privacy risk (Choi et al., 2025; Leschanowsky et al., 2024; Papneja & Yadav, 2025).

Prior research consistently identifies privacy concerns as a major barrier to information disclosure. According to privacy calculus theory, when individuals anticipate that disclosing personal information may lead to identity exposure, data misuse, or irreversible loss, they are more likely to be cautious, restrained, or even adopt avoidant behaviors (Dinev & Hart, 2006; Norberg et al., 2007; Yu et al., 2020). This mechanism is particularly relevant in generative AI contexts. Users often cannot clearly determine whether the system stores their inputs, how such information may be retrieved in subsequent interactions, or whether it may be used for model improvement, service optimization, or other secondary purposes. Furthermore, since generative AI is conversational by nature, disclosure is not a one-time event but an ongoing process that develops through continuous interaction (Leschanowsky et al., 2024; Choi et al., 2025). As a result, higher levels of Privacy Concern are likely to strengthen users' defensive behaviors, leading them to reduce the amount of sensitive input, limit the depth of their disclosures, or replace truthful disclosure with vague or incomplete statements. In other words, the more users worry that their personal information may be mishandled, the less likely they are to provide authentic, complete, or identifiable information to generative AI systems (Acquisti et al., 2015; Wang et al., 2023; Eitiveni et al., 2023).

Accordingly, the following hypothesis is proposed:

H1: Privacy Concern has a significant negative effect on Disclosure Intention.

2.2 Perceived Personalization Benefit and Disclosure Intention

Perceived Personalization Benefit refers to the functional, efficiency-related, and experiential value that users perceive based on a system's ability to recognize their needs, preferences, behavioral patterns, and contextual conditions. In generative AI contexts, such benefits are mainly reflected in more accurate answers, more relevant suggestions, more context-appropriate content generation, and greater problem-solving efficiency across learning, work, content creation, and decision support. Compared with conventional digital services, generative AI depends more heavily on the richness and specificity of user input to improve output quality. Therefore, users' subjective judgments regarding whether disclosing more information can produce better outcomes serve as a key basis for disclosure decision-making (Chakraborty et al., 2025; Choi et al., 2025).

Privacy calculus theory suggests that individuals are willing to disclose personal information under risky conditions because they expect to receive specific benefits in return (Dinev & Hart, 2006; Fernandes & Pereira, 2021). Existing studies likewise show that in recommendation systems, intelligent services, and personalized platforms, users are more willing to share information when they believe that doing so can substantially improve service relevance and their overall experience (Aguirre et al., 2015; Bol et al., 2018; Sutanto et al., 2013). In generative AI, this benefit mechanism is even more direct because the relevance, accuracy, and usefulness of system outputs often depend on whether users provide sufficient background, preference, and task-related information. When users believe that generative AI can effectively utilize their input to generate higher-quality, more relevant, and more personalized responses, disclosure is more likely to be viewed as a reasonable exchange of "information for value" rather than as mere exposure to risk (Chakraborty et al., 2025; Markou et al., 2025). Put differently, a stronger Perceived Personalization Benefit is likely to increase users' acceptance of disclosure and motivate them to provide more personal information to obtain more relevant and valuable interaction outcomes.

Accordingly, the following hypothesis is proposed:

H2: Perceived Personalization Benefit has a significant positive effect on Disclosure Intention.

2.3 Trust and Disclosure Intention

Trust refers to the psychological state in which users believe that generative AI systems and the platforms behind them are reliable, capable, and well-intentioned.

Users expect these systems to process personal information within reasonable boundaries, deliver stable services, and avoid intentionally harming their interests. In generative AI contexts, Trust encompasses not only judgments about system performance and output quality but also assessments of the platform's data-processing norms, privacy-protection capabilities, and overall predictability (McKnight et al., 2002; Gefen et al., 2003; Troshani et al., 2021). Furthermore, in algorithm-driven services, users' evaluations of system legitimacy, the rationality of processing rules, and the credibility of platform governance also shape their overall perceptions of the technology (Liu & Sun, 2024). Since users typically cannot directly observe internal system mechanisms or fully verify how their input data will be handled in subsequent processes, Trust becomes an essential basis for making disclosure decisions amid information asymmetry (Joinson et al., 2010; Leschanowsky et al., 2024).

Trust functions as a key mechanism for reducing uncertainty and mitigating perceived vulnerability. A substantial body of research shows that Trust significantly promotes technology adoption, continued use, and collaborative behavior, and increases individuals' tolerance for potential risks in high-uncertainty environments (Pavlou, 2003; Gefen et al., 2008; Liu & Tao, 2022). In broader research on intelligent interaction, users' trust in AI or robotic systems is likewise regarded as a crucial prerequisite for acceptance and cooperation (Ding & Zhou, 2025). In the case of generative AI, users often find it difficult to fully understand how outputs are produced or to determine whether their personal information will be handled appropriately. Under such circumstances, objective knowledge alone is insufficient to support active disclosure decisions. Trust provides a form of relational assurance, enabling users to develop a general expectation that the system is reliable despite incomplete information. When this expectation is strong, users are more likely to reduce concerns about misuse, leakage, and loss of control. Consequently, they may provide more authentic and detailed personal information in exchange for better service performance (Lappeman et al., 2023; Markou et al., 2025; Yu et al., 2025). By contrast, when users lack basic Trust in the system and the platform that supports it, they are more likely to strengthen self-protective tendencies, which can suppress their intention to disclose information (Joinson et al., 2010; Liu & Tao, 2022).

Accordingly, the following hypothesis is proposed:

H3: Trust has a significant positive effect on Disclosure Intention.

3. Method

3.1 Data Collection and Sample

This study employed a questionnaire survey to collect data, and the valid responses served as the basis for the empirical analysis. After data screening, a total of 302 valid responses were retained. The demographic characteristics of the respondents and the distribution of generative AI usage behavior are presented in Table 1.

In terms of demographic characteristics, the sample was predominantly female, with women accounting for 70.53% of respondents and men accounting for 29.47%. The age distribution was concentrated in younger groups: respondents aged 18–25 accounted for 50.66%, and those aged 26–35 accounted for 40.40%, together representing 91.06% of the sample. Respondents aged 36 and above made up a relatively small proportion. Monthly income was relatively dispersed: 36.42% of respondents earned 3,000 yuan or less, 23.51% earned 3,001–5,000 yuan, and the combined proportion of those earning more than 5,000 yuan was 40.07%. In terms of educational attainment, respondents with a bachelor's degree accounted for the largest proportion at 38.41%, followed by those with a high school education or below at 33.11%, while junior college graduates and those with a master's degree or above accounted for 20.53% and 7.95%, respectively.

Regarding generative AI usage behavior, 23.84% of respondents reported that they had never used generative AI, whereas 76.16% had prior experience with it. Among all respondents, 64.91% reported using generative AI at least once per week, indicating that most participants had at least some degree of exposure to and experience with generative AI. In terms of primary usage scenarios, generative AI was mainly used for learning/research (42.05%) and work/office tasks (38.08%), which together accounted for 80.13% of the sample. By contrast, the proportions of respondents using generative AI for daily life consultation and creative writing/content generation were relatively low, at 14.24% and 5.63%, respectively.

During data collection, this study adhered to the basic requirements of research ethics. Before the questionnaire was distributed, respondents were informed of the study purpose, response procedures, and intended use of the data. All respondents participated voluntarily and provided informed consent. The questionnaire was administered anonymously and did not collect personally identifiable information. All data were used exclusively for academic research purposes.

Table 1. Demographic Characteristics of the Respondents and Distribution of Generative AI Usage Behavior

Variable	Category	Frequency	Percentage (%)	Cumulative Percentage (%)
Gender	Male	89	29.47	29.47
	Female	213	70.53	100.00
Age	18–25 years	153	50.66	50.66
	26–35 years	122	40.40	91.06
	36–45 years	21	6.95	98.01
	46 years and above	6	1.99	100.00
Monthly Income	3000 yuan or less	110	36.42	36.42
	3001-5000 yuan	71	23.51	59.93
	5001-8000 yuan	39	12.91	72.85
	8,001–12,000 yuan	41	13.58	86.42
	12,001 yuan and above	41	13.58	100.00
Education Level	High school and below	100	33.11	33.11
	junior college education	62	20.53	53.64
	undergraduate course	116	38.41	92.05
	Master’s degree or above	24	7.95	100.00
Frequency of Using Generative AI (e.g., ChatGPT, Wenxin Yiyan, Tongyi Qianwen)	Never used	72	23.84	23.84
	1-2 times per month	34	11.26	35.10
	1-2 times per week	49	16.23	51.32
	3-5 times per week	68	22.52	73.84
	1-2 times per day	44	14.57	88.41
	Several times a day	35	11.59	100.00
Primary Usage Scenario of Generative AI	Learning/Research	127	42.05	42.05
	Work/Office	115	38.08	80.13
	Daily Life Counseling	43	14.24	94.37
	Creative Writing/Content Generation	17	5.63	100.00
Total		302	100.0	100.0

3.2 Scale Design

The questionnaire consisted of two parts. The first part collected respondents' demographic information, including gender, age, monthly income, educational level, frequency of generative AI use, and primary usage scenarios. The second part measured the core constructs in the study, namely Privacy Concern, Perceived Personalization Benefit, Trust, and Disclosure Intention.

In terms of scale design, Privacy Concern was measured using five items, focusing on respondents' concerns about the unauthorized collection and use of personal information by generative AI, the possibility of personal data being leaked to third parties, loss of control over the content they input, the use of information for purposes they do not understand or agree with, and the overall security of personal information disclosure.

Perceived Personalization Benefit was measured using four items, focusing on whether disclosing personal information could lead to responses that better fit users' needs, more precise and personalized service experiences, higher-quality content generation, and whether such personalized benefits justify disclosure.

Trust was measured using four items that assessed respondents' confidence in the reliability of generative AI, its ability to handle information as promised, its capacity to protect users' information, and the overall security of its data-processing practices.

Disclosure Intention was measured using three items that captured respondents' current and future intentions to disclose personal information to generative AI.

The items for each construct were coded as PC1–PC5, PPB1–PPB4, TRU1–TRU4, and DI1–DI3, respectively. All core variables were measured on a five-point Likert scale, where 1 = "strongly disagree," 2 = "disagree," 3 = "neutral," 4 = "agree," and 5 = "strongly agree." Higher scores indicate stronger cognitive evaluations or behavioral tendencies with respect to the corresponding construct.

The questionnaire items were adapted primarily from established scales and revised to fit the context of generative AI usage. Specifically, the Privacy Concern scale was adapted from Malhotra et al. (2004), the Perceived Personalization Benefit scale was adapted from Dinev and Hart (2006), the Trust scale was adapted from McKnight, Choudhury, and Kacmar (2002), and the Disclosure Intention scale was adapted from Xu et al. (2011).

3.3 Pre-test

To ensure that the questionnaire aligns with the research objectives, and is clear and understandable, this study conducted a content review and revision before the formal survey was administered. The revision process focused on several key aspects: the dimensional structure of each construct was clearly defined, the wording of the items matched generative AI usage contexts, different constructs were conceptually distinguishable, and the overall measurement logic was internally consistent. This approach of adapting well-established scales to a new technological context is consistent with common practices in information privacy and technology behavior research (Malhotra et al., 2004; McKnight et al., 2002; Xu et al., 2011).

Given the study's focus on personal information disclosure in generative AI contexts, the questionnaire revision centered on four key constructs: Privacy Concern, Perceived Personalization Benefit, Trust, and Disclosure Intention. Specifically, the wording, meaning, and context of several items were refined to avoid overly abstract, lengthy, or ambiguous expressions. This revision aimed to improve the clarity and consistency with which respondents understood the questionnaire items.

Before the formal survey was launched, the questionnaire instructions, item order, and response procedures were also carefully reviewed to ensure a clear completion process and smooth administration. After the revisions were finalized, the formal questionnaire was developed, and data collection began. In the formal analysis stage, reliability, exploratory factor, correlation, and regression analyses were conducted to evaluate the quality of the scales and the relationships among variables.

4. Findings

4.1 Reliability and Validity Testing

1) Reliability Testing

As shown in Table 2, the Cronbach's α coefficients for each construct ranged from 0.820 to 0.871, all exceeding the commonly accepted threshold, indicating good internal consistency of the scale. Specifically, the Cronbach's α for privacy concerns was 0.871, perceived personalized benefits was 0.836, trust was 0.864, and willingness to disclose personal information to generative AI was 0.820 (see Table 2). Overall, the reliability levels of all constructs met the requirements for subsequent analysis.

Table 2. Reliability Test Results of Each Scale

Construct	Number of Items	Cronbach's a
Privacy Concern	5	0.871
Perceived Personalization Benefit	4	0.836
Trust	4	0.864
Disclosure Intention	3	0.820

2) Exploratory Factor Analysis

Prior to conducting the exploratory factor analysis, the data were first examined for factor analysis fit. The results showed a KMO value of 0.876, and the Bartlett's test for sphericity was significant (χ^2 = 2245.209, df = 120, p <0.001), indicating that the correlation matrix was not an identity matrix and that the sample data were suitable for factor analysis (see Table 3).

Table 3. KMO and Bartlett's Test Results

KMO and Bartlett's tests		
KMO		0.876
Bartlett's Test of Sphericity	Approximate Chi-square	2245.209
	df	120
	p-value	0.000

Further analysis revealed that four common factors with eigenvalues greater than 1 were extracted. Before rotation, the cumulative variance explained by these four factors was 69.352%; after rotation, the cumulative variance explained remained at 69.352%, with each factor being 20.655%, 17.980%, 16.987%, and 13.731%, respectively. These results indicate that the extracted factors adequately account for the variance in the original measurement items (see Table 4).

Table 4. Total Variance Explained in the Exploratory Factor Analysis

Factor number	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Eigenvalue	Variance Explained (%)	Cumulative (%)	Eigenvalue	Variance Explained (%)	Cumulative (%)	Eigenvalue	Variance Explained (%)	Cumulative (%)
1	5.698	35.610	35.610	5.698	35.610	35.610	3.305	20.655	20.655
2	2.245	14.031	49.641	2.245	14.031	49.641	2.877	17.980	38.635
3	1.825	11.403	61.044	1.825	11.403	61.044	2.718	16.987	55.621
4	1.329	8.308	69.352	1.329	8.308	69.352	2.197	13.731	69.352

Factor number	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Eigenvalue	Variance Explained (%)	Cumulative (%)	Eigenvalue	Variance Explained (%)	Cumulative (%)	Eigenvalue	Variance Explained (%)	Cumulative (%)
5	0.566	3.537	72.889						
6	0.533	3.332	76.222						
7	0.493	3.083	79.304						
8	0.473	2.957	82.262						
9	0.449	2.809	85.071						
10	0.412	2.573	87.643						
11	0.387	2.418	90.061						
12	0.361	2.258	92.320						
13	0.337	2.106	94.426						
14	0.331	2.070	96.496						
15	0.301	1.880	98.375						
16	0.260	1.625	100.000						

The rotated factor loading matrix reveals high loadings for each item on its respective factor, with no significant cross-loading observed. Items demonstrate a commonality coefficient ranging from 0.637 to 0.762. Overall, the measurement items exhibit strong construct validity, showing clear differentiation between constructs, indicating the scale possesses robust structural validity (see Table 5).

Table 5. Rotated Factor Loadings and Communalities

Item	Factor Loading Coefficient				Communality
	Factor 1	Factor 2	Factor 3	Factor 4	
PC1	0.785				0.690
PC2	0.771				0.639
PC3	0.764				0.637
PC4	0.788				0.695
PC5	0.788				0.657
PPB1			0.806		0.692
PPB2			0.779		0.646
PPB3			0.789		0.670
PPB4			0.824		0.713
TRU1		0.817			0.694
TRU2		0.822			0.721
TRU3		0.781			0.700
TRU4		0.821			0.738
DI1				0.822	0.762
DI2				0.796	0.726
DI3				0.790	0.717

4.2 Correlation Analysis

Table 6 presents the mean values, standard deviations, and correlation coefficient matrix of the variables. The descriptive statistics indicate that the perceived benefits of personalization have the highest mean value (M = 3.839, SD = 0.968), followed by willingness to disclose personal information to generative AI (M = 3.731, SD = 1.083) and trust (M = 3.716, SD = 1.044), while privacy concerns show a relatively lower mean value (M = 2.366, SD = 1.037).

The correlation analysis revealed that willingness to disclose personal information to generative AI was significantly positively correlated with perceived personalized benefits ($r = 0.320$, $p < 0.001$) and trust ($r = 0.434$, $p < 0.001$), while showing a significant negative correlation with privacy concerns ($r = -0.419$, $p < 0.001$). Meanwhile, privacy concerns were significantly negatively correlated with both perceived personalized benefits ($r = -0.328$, $p < 0.001$) and trust ($r = -0.382$, $p < 0.001$). A significant positive correlation was also observed between perceived personalized benefits and trust ($r = 0.193$, $p < 0.001$). Overall, the correlation directions among variables aligned with theoretical expectations, providing preliminary evidence for subsequent regression analysis.

Table 6. Descriptive Statistics and Correlation Matrix

	Average value	Standard error	Disclosure Intention	Privacy Concern	Perceived Personalization Benefit	Trust
Disclosure Intention	3.731	1.083	1			
Privacy Concern	2.366	1.037	-0.419***	1		
Perceived Personalization Benefit	3.839	0.968	0.320***	-0.328***	1	
Trust	3.716	1.044	0.434***	-0.382***	0.193***	1
* p<0.05 ** p<0.01 *** p<0.001						

4.3 Regression Analysis

To examine the effects of Privacy Concern, Perceived Personalization Benefit, and Trust on Disclosure Intention, this study constructed a multiple linear regression model with Disclosure Intention as the dependent variable. The results showed that the overall model was significant ($F(3, 298) = 41.058$, $p < 0.001$), and the adjusted R^2 was 0.285, indicating that the three predictor variables jointly explained 28.5% of the variance in Disclosure Intention (Table 7).

The model diagnostics further showed that the variance inflation factor (VIF) values of all predictors ranged from 1.127 to 1.271, and all tolerance values were above 0.70, indicating no serious multicollinearity problem. In addition, the Durbin–Watson statistic was 2.090, suggesting that the residuals were not significantly autocorrelated and that the model estimates were robust.

Regarding the specific regression results, Privacy Concern had a significant negative effect on Disclosure Intention ($\beta = -0.242$, $t = -4.406$, $p < 0.001$), whereas Perceived Personalization Benefit ($\beta = 0.182$, $t = 3.510$, $p = 0.001$) and Trust ($\beta = 0.306$, $t = 5.794$, $p < 0.001$) both had significant positive effects on Disclosure Intention. A comparison of the standardized regression coefficients showed that Trust had the strongest explanatory power, followed by Privacy Concern, while Perceived Personalization Benefit had the weakest effect among the three predictors. These findings indicate that Trust is the most important promoting factor in explaining users' Disclosure Intention toward generative AI, whereas Privacy Concern is a significant inhibiting factor. Thus, H1, H2, and H3 were all supported.

Table 7. Multiple Regression Results for Disclosure Intention

Results of linear regression analysis

	Nonstandardized Coefficient		Standardized Coefficient	t	p	Collinearity Diagnostics	
	B	SE	Beta			VIF	Tolerance
constant	2.368	0.375	-	6.308	0.000***	-	-
Privacy Concern	-0.253	0.057	-0.242	-4.406	0.000***	1.271	0.787
Perceived Personalization Benefit	0.203	0.058	0.182	3.510	0.001***	1.127	0.887
Trust	0.318	0.055	0.306	5.794	0.000***	1.178	0.849
R^2	0.292						
Adjusted R^2	0.285						
F	F (3,298)=41.058,p=0.000						
Durbin–Watson	2.090						
Dependent variable = Willingness to disclose personal information to generative AI							
* p<0.05 ** p<0.01 *** p<0.001							

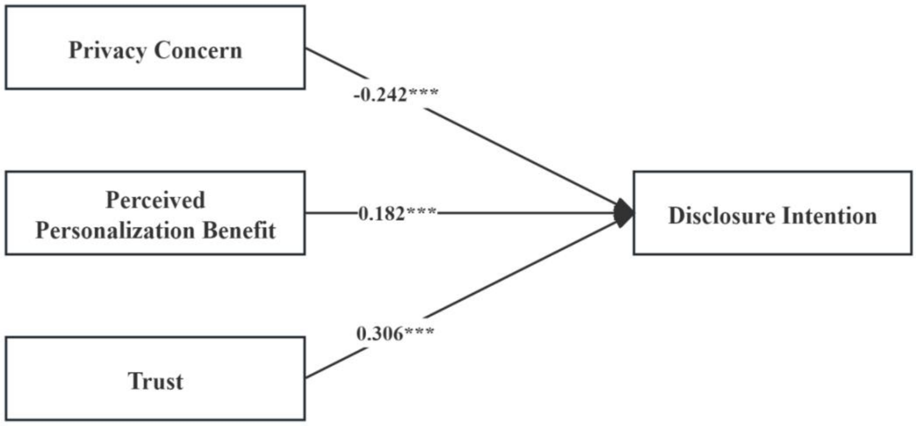

Figure 1. Effects of Privacy Concern, Perceived Personalization Benefit, and Trust on Disclosure Intention in Generative AI Contexts

5. Discussion

5.1 Key Findings

This study empirically examined the formation of Disclosure Intention in generative AI contexts. It focused on the effects and explanatory power of three core factors: Privacy Concern, Perceived Personalization Benefit, and Trust. The results showed that all three variables were significantly associated with users' Disclosure Intention, and the direction of these effects aligned with theoretical expectations. Specifically, Privacy Concern had a significant negative effect on Disclosure Intention, whereas Perceived Personalization Benefit and Trust both had significant positive effects. These findings suggest that, in generative AI contexts, users' Disclosure Intention depends on their overall evaluation of potential risks, expected benefits, and relational assurance. This result is consistent with the core logic of privacy calculus theory, which conceptualizes disclosure as a trade-off between perceived risks and expected benefits, and is also consistent with prior research on online privacy and information disclosure (Dinev & Hart, 2006; Dienlin & Metzger, 2016; Fernandes & Pereira, 2021; Yu et al., 2020; Eitiveni et al., 2023).

A further analysis of the standardized regression coefficients showed that Trust had the strongest explanatory power among the three predictors, followed by Privacy Concern, whereas Perceived Personalization Benefit had the weakest effect. This finding indicates that in generative AI environments characterized by high uncertainty and unclear technical mechanisms, Trust is more influential than benefit expectation alone in supporting users' Disclosure Intention. In other words, although Perceived Personalization Benefit can enhance users' willingness to disclose information, a lack of basic Trust in the system and the platform behind it may still substantially inhibit disclosure. By contrast, when users perceive that the system is reliable, capable of handling personal information appropriately, and unlikely to cause harmful consequences, they are more likely to engage in information exchange. This result is consistent with prior studies in online environments and intelligent services, which show that Trust promotes cooperation and reduces perceived uncertainty (McKnight et al., 2002; Gefen et al., 2003; Pavlou, 2003; Lappeman et al., 2023; Ding & Zhou, 2025).

The correlation analysis also showed that Privacy Concern was significantly and negatively associated with Disclosure Intention, whereas Perceived Personalization Benefit and Trust were significantly and positively associated with Disclosure Intention. In addition, Privacy Concern was significantly related to both Trust and Perceived Personalization Benefit. This suggests that disclosure in generative AI contexts is not driven by a single isolated factor; rather, it reflects a combination of elements. Specifically, it involves risk inhibition, benefit motivation, and relational assurance. Overall, the findings provide a clear empirical basis for understanding user behavior regarding data-related generative AI contexts and offer a direct response to the research questions proposed in this study (Choi et al., 2025; Papneja & Yadav, 2025).

5.2 Theoretical Contributions

The theoretical contributions of this study are reflected in three main aspects.

First, this study extends research on personal information disclosure to the emerging interactive context of generative AI. Unlike traditional e-commerce, social media, or general online platforms, disclosure in generative AI is more conversational, continuous, and context-embedded. Users' inputs often develop progressively over the course of task completion. By exploring disclosure behavior in this new technological setting, the study expands the application of existing disclosure research. It helps move the literature beyond relatively static, authorization-based models toward a more dynamic and interaction-centered perspective (Papneja & Yadav, 2025; Choi et al., 2025; Leschanowsky et al., 2024).

Second, this study develops an integrated framework that combines Privacy Concern, Perceived Personalization Benefit, and Trust into a unified explanatory model. Existing studies have often emphasized privacy-related risk, personalization-related benefit, or technological trust separately. However, this study shows that users' Disclosure Intention in generative AI contexts cannot be adequately explained by risk avoidance or benefit seeking alone, but instead emerges from the combined influence of these three variables. In this sense, the study improves the theoretical integration of disclosure research in generative AI settings (Dinev & Hart, 2006; Fernandes & Pereira, 2021; Smith et al., 2011; Eitiveni et al., 2023).

Third, beyond testing the significance of the three antecedents, this study further compares their relative explanatory power. The finding that Trust has the strongest explanatory role suggests that relational assurance is important in generative AI contexts, where users depend heavily on technological intermediaries and system judgments. This result enriches the application of privacy calculus theory in generative AI settings and indicates that future research should not view disclosure merely as a simple risk–benefit trade-off. Instead, greater attention should be given to the foundational role of Trust in shaping user decisions under conditions of high uncertainty (Gefen et al., 2008; McKnight et al., 2002; Liu & Tao, 2022; Liu & Sun, 2024).

5.3 Practical Implications

Based on the empirical findings and the specific characteristics of generative AI interaction contexts, this study offers the following practical implications.

First, platforms should regard the reduction of privacy concerns as a crucial prerequisite for enhancing Disclosure Intention. This means that platforms should not rely solely on users' desire for convenience to encourage them to provide information. Instead, they should work to reduce concerns about loss of control over information, potential leakage, and misuse. This can be achieved through clearer privacy policy communication, more explicit explanations of data usage, more transparent permission settings, and more visible warnings about sensitive information. In particular, in multi-turn dialogue contexts, platforms should help users identify content that may involve sensitive information and provide clearer prompts regarding the boundaries of appropriate disclosure. This recommendation aligns with prior privacy research emphasizing the importance of institutional safeguards, information control, and privacy notice mechanisms (Acquisti et al., 2015; Xu et al., 2011; Bélanger & Crossler, 2011).

Second, platforms need to communicate the Perceived Personalization Benefit effectively, and those benefits should be clear and understandable to users. The findings indicate that Perceived Personalization Benefit significantly increases Disclosure Intention, which suggests that users are not inherently resistant to sharing information; rather, they evaluate whether disclosure is worthwhile. Therefore, platforms can enhance users' sense of value by improving response accuracy, enhancing task relevance, and optimizing contextual adaptation to individual needs. However, the presentation of personalization benefits should not rely on vague or excessive data collection practices. Instead, it should remain closely aligned with users' task goals to avoid the emergence of distrust. This implication is consistent with prior research on the personalization–privacy paradox (Aguirre et al., 2015; Aguirre et al., 2016; Bol et al., 2018; Sutanto et al., 2013).

Third, platforms should prioritize Trust in their governance and design strategies. The present study found that Trust had the strongest explanatory power among the three predictors, indicating that users' Disclosure Intention in generative AI contexts depends to a large extent on whether they regard the system and the platform as reliable. Therefore, platforms should not focus solely on model capabilities; they should also cultivate Trust through responses, consistent explanations, transparency in information processing, error-correction mechanisms, and clear signals of responsibility. In other words, what ultimately sustains disclosure and cooperation is not just functional performance but also the credible image established through long-term interaction. Platforms should also consider users' broader perceptions of algorithmic procedures, decision legitimacy, and governance norms to strengthen stable relational expectations toward the system (McKnight et al., 2002; Troshani et al., 2021; Yu et al., 2025; Liu & Sun, 2024).

5.4 Limitations and Future Research

Although this study provides an initial empirical examination of the determinants of Disclosure Intention in generative AI contexts, several limitations should be acknowledged.

First, this study used cross-sectional questionnaire data. As a result, the relationships among variables were interpreted primarily in terms of statistical association rather than strict causal identification. Future research could adopt longitudinal designs, experiments, or scenario-based manipulations to more rigorously examine the dynamic effects of Privacy Concern, Perceived Personalization Benefit, and Trust on Disclosure Intention.

Second, the core variables in this study were measured through self-reported responses, which may be subject to common method bias and subjective evaluation bias. Although the reliability and structural validity results were generally satisfactory, future research could incorporate behavioral data, simulated scenarios, or platform usage records to measure actual disclosure behavior more directly, thereby improving the behavioral validity of the findings. This approach is also consistent with prior discussions about the gap between disclosure intention and actual disclosure behavior in privacy research (Norberg et al., 2007).

Third, the sample consisted primarily of younger respondents and included a relatively high proportion of women. In addition, some respondents had not previously used generative AI. Accordingly, the measured Disclosure Intention reflects both the behavior of actual users and the attitude of potential users. Future research could more clearly distinguish between experienced and inexperienced users, conduct subgroup comparisons or robustness tests, and replicate the findings across samples with different ages, occupations, and cultural backgrounds to improve external validity and generalizability (Wang et al., 2023).

Finally, this study focused primarily on three key factors—Privacy Concern, Perceived Personalization Benefit, and Trust. However, disclosure behavior in generative AI contexts may also be shaped by additional factors, such as algorithmic transparency, platform reputation, task sensitivity, usage purpose, AI literacy, and perceived regulation. Future studies could expand the framework developed here by examining mediating mechanisms, moderating effects, and contextual differences, thereby building a more comprehensive explanatory model of disclosure in generative AI settings (Leschanowsky et al., 2024; Papneja & Yadav, 2025).

6. Conclusion

As generative AI rapidly becomes increasingly integrated into everyday life and professional settings, users' Disclosure Intention has emerged as an important issue for understanding intelligent interaction behavior and managing platforms effectively. Based on questionnaire data, this study systematically examined the impact of Privacy Concern, Perceived Personalization Benefit, and Trust on Disclosure Intention in generative AI contexts. The results showed that Privacy Concern had a significant negative effect on Disclosure Intention, whereas Perceived Personalization Benefit and Trust had significant positive effects. Among the three factors, Trust demonstrated the strongest explanatory power based on the absolute values of the standardized regression coefficients. These findings indicate that disclosure in generative AI contexts is not merely a simple balancing of cost and benefits, but rather the result of the combined influence of risk perception, expected benefits, and relational assurance. The study further suggests that, in order to enhance users' willingness to cooperate and disclose information in generative AI environments, platforms should not rely solely on technical performance or service convenience. Instead, they should simultaneously strengthen privacy risk governance, clearly communicate the value of personalization, and build Trust. Overall, this study provides initial empirical evidence for understanding disclosure in generative AI contexts and offers a useful analytical framework for future research and platform practices.

Funding: Not applicable.

Acknowledgments: Not applicable.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data are not publicly available due to privacy and ethical restrictions but are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing*, 33(2), 98–110. https://doi.org/10.1108/JCM-06-2015-1458

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041. https://doi.org/10.2307/41409971

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., ... & De Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, 23(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Chakraborty, D., Gunasekaran, A., & Subramanian, G. (2025). Privacy vs. personalization: GENAI's role in technology adoption. *Journal of Computer Information Systems*, 1–18. https://doi.org/10.1080/08874417.2025.2534545

Choi, Y., Zhunis, A., Dong, W., Seering, J., Park, S., Cha, M., & Chin, H. (2025). Privacy disclosure to large language models: A large-scale study on awareness, benefits, and concerns in health contexts across three countries. *Computers in Human Behavior Reports*, 20, 100841. https://doi.org/10.1016/j.chbr.2025.100841

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, 21(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Ding, X., & Zhou, Y. (2025). A study of factors influencing user trust in human-robot interaction. *Journal of Arts and Cultural Studies*, 4(2), 1–19. https://doi.org/10.23112/acs25073101

Eitiveni, I., Hidayanto, A. N., Dwityafani, Y. A., & Kumaralalita, L. (2023). Self-disclosure on professional social networking sites: A privacy calculus perspective. *Human Behavior and Emerging Technologies*, 2023(1), 2643683. https://doi.org/10.1155/2023/2643683

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, 65, 101717. https://doi.org/10.1016/j.tele.2021.101717

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems*, 24(4), 275–286. https://doi.org/10.2753/MIS0742-1222240411

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90. https://doi.org/10.2307/30036519

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, 25(1), 1–24. https://doi.org/10.1080/07370020903586662

Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2023). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing*, 28(2), 337–357. https://doi.org/10.1057/s41264-022-00154-z

Leschanowsky, A., Rech, S., Popp, B., & Bäckström, T. (2024). Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review. *Computers in Human Behavior*, 159, 108344. https://doi.org/10.1016/j.chb.2024.108344

Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, 127, 107026. https://doi.org/10.1016/j.chb.2021.107026

Liu, Y., & Sun, X. (2024). Towards more legitimate algorithms: A model of algorithmic ethical perception, legitimacy, and continuous usage intentions of e-commerce platforms. *Computers in Human Behavior*, 150, 108006. https://doi.org/10.1016/j.chb.2023.108006

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Markou, V., Serdaris, P., Antoniadis, I., & Spinthiropoulos, K. (2025). Personalization, trust, and identity in AI-based marketing: An empirical study of consumer acceptance in Greece. *Administrative Sciences*, 15(11), 440. https://doi.org/10.3390/admsci15110440

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Papneja, H., & Yadav, N. (2025). Self-disclosure to conversational AI: A literature review, emergent framework, and directions for future research. *Personal and Ubiquitous Computing*, 29(2), 119–151. https://doi.org/10.1007/s00779-024-01823-7

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015. https://doi.org/10.2307/41409970

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization–privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 37(4), 1141–1164. https://doi.org/10.25300/MISQ/2013/37.4.07

Troshani, I., Rao Hill, S., Sherman, C., & Arthur, D. (2021). Do we trust in AI? Role of anthropomorphism and intelligence. *Journal of Computer Information Systems*, 61(5), 481–491. https://doi.org/10.1080/08874417.2020.1788473

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546–562. https://doi.org/10.1509/jmr.10.0355

Wang, N., Zhao, Y., Zhou, R., & Li, Y. (2023). Factors influencing users' online information disclosure intention and the moderating effect of cultural background and platform type. *Aslib Journal of Information Management*, 75(6), 1178–1208. https://doi.org/10.1108/AJIM-04-2022-0218

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798–824. https://doi.org/10.17705/1jais.00281

Yu, L., Li, H., He, W., Wang, F. K., & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51, 102015. https://doi.org/10.1016/j.ijinfomgt.2019.09.011

Yu, T., Tian, Y., Chen, Y., Huang, Y., Pan, Y., & Jang, W. (2025). How do ethical factors affect user trust and adoption intentions of AI-generated content tools? *Evidence from a risk-trust perspective. Systems*, 13(6), 461. https://doi.org/10.3390/systems13060461

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, 56(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001