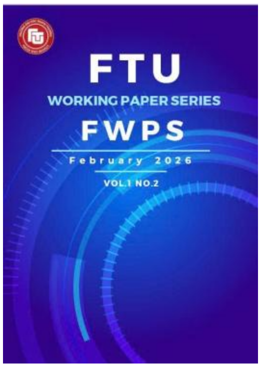

Working Paper 2026.1.2.19

- Vol. 1, No. 2

PHÉP TÍNH QUYỀN RIÊNG TƯ TRONG CÁC HỆ THỐNG GỢI Ý DỰA TRÊN NỘI DUNG: VAI TRÒ ĐIỀU TIẾT CỦA TÍNH MINH BẠCH TRONG VIỆC ĐỊNH HÌNH NHẬN THỨC CỦA NGƯỜI DÙNG VỀ RỦI RO VÀ LỢI ÍCH

Trần Khánh Ngọc[1], Trần Thị Hải Yến, Nguyễn Cao Thùy Linh,

Nguyễn Vân Anh

Sinh viên K63 CTTT Kinh tế đối ngoại – Viện Kinh tế và Kinh doanh quốc tế

Trường Đại học Ngoại Thương, Hà Nội, Việt Nam

Phạm Thị Cẩm Anh

Giảng viên Viện Kinh tế và Kinh doanh quốc tế

Trường Đại học Ngoại thương, Hà Nội, Việt Nam

Tóm tắt

Trong bối cảnh hệ thống gợi ý dựa trên nội dung trên mạng xã hội, nghiên cứu phân tích mối quan hệ giữa mức độ cá nhân hóa và sự sẵn lòng tiết lộ dữ liệu của người dùng, đồng thời nhấn mạnh vai trò điều tiết của tính minh bạch trong các đề xuất nội dung. Dựa trên lý thuyết tính toán quyền riêng tư, mô hình nghiên cứu được kiểm định với dữ liệu khảo sát từ 287 người dùng mạng xã hội. Kết quả cho thấy cá nhân hóa được cảm nhận làm gia tăng đáng kể cả lợi ích cảm nhận và rủi ro cảm nhận, phù hợp với các nghiên cứu trước đây. Lợi ích cảm nhận có tác động tích cực đến sự sẵn lòng tiết lộ dữ liệu, trong khi rủi ro cảm nhận có ảnh hưởng tiêu cực. Mô hình giải thích ở mức trung bình phương sai của lợi ích cảm nhận và ở mức khiêm tốn đối với sự sẵn lòng tiết lộ, trong khi khả năng giải thích đối với rủi ro cảm nhận còn hạn chế. Đáng chú ý, tính minh bạch thể hiện vai trò điều tiết: khi mức độ minh bạch cao, tác động tích cực của cá nhân hóa lên lợi ích cảm nhận được tăng cường, đồng thời tác động của cá nhân hóa lên rủi ro cảm nhận suy giảm. Nghiên cứu đóng góp vào mô hình bằng cách giới thiệu khái niệm tính minh bạch như một yếu tố điều tiết, do đó cung cấp những hiểu biết quan trọng cho người dùng mạng xã hội và nhà phát triển nền tảng.

---

[1] Tác giả liên hệ, Email: k63.2412140085@ftu.edu.vn

Từ khóa: cá nhân hóa, quyền riêng tư, tiết lộ dữ liệu, tính minh bạch, hệ thống đề xuất dựa trên nội dung

THE PRIVACY CALCULUS OF CONTENT-BASED RECOMMENDATION SYSTEMS: THE MODERATING ROLE OF TRANSPARENCY IN SHAPING USER'S PERCEPTION OF RISKS AND BENEFITS

Abstract

This study examines the relationship between personalization features and willingness to disclose data in the context of content-based recommendation system, and the moderating role of transparency in this relationship. The authors applied the privacy calculus theory with the use of a structural equation approach and survey data of 278 social media users. The results are consistent with prior literature as they indicate that perceived personalization significantly increases perceived benefit and perceived risk. These results propose that perceived benefit has a positive influence on willingness to disclose data, whereas perceived risk demonstrates a negative effect. The model accounts for a moderate amount of variance in perceived benefit, and a modest amount in willingness to disclose; however, remaining limited explanatory power for perceived risk. Notably, transparency shows a significant moderating role in the studied relationships. Specifically, a higher level of transparency amplifies the positive effect of personalization on perceived benefits, while weakening its relationship with perceived risks. The study contributes to the privacy calculus framework by introducing the concept of transparency as a moderator, therefore providing significant inssights for both social media users and platform developers.

Keywords: personalization, privacy, data disclosure, transparency, content-based recommendation systems

1. Introduction

Nowadays, social media plays a significant part of the digital life. By 2025, the global population of active social media users will exceed 5.24 billion people, representing 63.9 percent of the global population (We are Social, 2025). This high growth rate of digital information has increased the creation and application of new sophisticated personalization technologies, especially Content-Based Recommendation Systems (CBRS). Even though CBRS relies on personal data and retains understandable processes, such a high level of personalization necessitates extensive processing and gathering of personal data, which brings the issue of privacy, security of personal data, and trust in recommendation systems. More than 70% of internet users worry about the misuse of their personal data (Statista, 2025), and 76% refuse to purchase online if businesses fail to protect consumer privacy (Trūata, 2021). These results demonstrate the increasing tension between the users' needs and individual services, and their rising concerns regarding the protection of privacy.

This tension is explained through the privacy calculus framework, which suggests that individuals decide whether to disclose personal information after weighing perceived benefits against perceived risks. Within recommendation systems, users may perceive benefits such as relevance, convenience, and efficiency, while simultaneously perceiving risks related to data misuse, surveillance, or loss of control. The data disclosure decision-making process of CBRS is becoming more complicated as it incorporates tremendous aspects of artificial intelligence (AI), which reinforces the relevance of the privacy calculus framework in the domain.

Prior research on the personalization-privacy paradox provides important foundations for understanding privacy calculus in personalized digital environments. Using SEM and LISREL on a sample of 523 respondents, Awad and Krishnan (2006) find that when consumers perceive visible benefits from personalization, prior privacy invasion concerns become insignificant in decision making. The study also indicates that consumers who prioritize information transparency are less willing to be profiled.

Extending the privacy calculus to location-aware marketing, Xu et al. (2011)'s research, based on survey data from 545 mobile users, shows that covert location-aware marketing exerts stronger effects across relationships and is more likely to trigger spontaneous purchases compared to overt ones. More recently, Cloarec et al. (2024) further revealed that trust beliefs marginally increase willingness to disclose, while information collection concerns marginally decrease it. Both trust beliefs and information collection concerns moderate the relationship between posting frequency and willingness to disclose, therefore confirming the transformative nature of the privacy calculus.

Similarly, Tintarev and Masthoff (2012) posit providing transparent explanations improves user assessment of benefit and risk. By increasing perceived utility and reducing privacy concerns about data misuse, transparent explanations not only enhance effectiveness – by helping users identify their preferred content – and scrutability – by enabling users to understand and validate the internal logic of recommendation systems. Therefore, these mechanisms help reduce uncertainty while increasing perceived values of social media users. Despite significant contributions to the framework, these research remains insufficient to address the active role of users in privacy setting management, highlighting the need for future studies in the context of CBRS.

Incorporating the framework of privacy calculus in personalization contexts, this paper aims to explore the influence of perceived personalization on individuals' willingness to disclose data. Specifically, the study (1) examines how perceived personalization shapes the willingness to disclose data, (2) analyze the mediated effect of perceived benefits and perceived risks on data disclosure intentions, and (3) assess the moderating role of transparency in these relationships. The study is expected to extend the privacy calculus framework to the field of personalization systems, therefore providing practical insights for users and developers in balancing perceived benefits and risks of customized features.

2. Theoretical Framework and Hypotheses

Personalization can be defined as tailoring content, services or information to specific individual in accordance with their personal data and preferences (Chellappa & Sin, 2005; Strycharz et al., 2019). In recommendation system contexts, personalization is defined through the analysis of content-tailored features on social media, such as text, images, or user-engaged posts, to capture users' preferences. It captures users' subjective assessment of the relevance and individual fit of the recommended content. In this paper, perceived personalization is the subjective evaluation of relevance and personal fit of the recommended content by the users.

2.1. Underpinning Theories

2.1.1. Personalization - Privacy Paradox

The personalization-privacy paradox reflects the tension between the benefits of customized services and the risks of data exploitation, where excessive privacy concerns can lead to a significant reduction in user engagement (Aguirre et al., 2015; Awad & Krishnan, 2006; Cloarec et al., 2021). While AI-driven systems like CBRS enhance satisfaction through personalization features, they simultaneously intensify the fear of privacy misuse due to the "black-box" nature of advanced algorithms and the users' limited control over data processing (Bojić et al., 2022; Zhang et al., 2021).

2.1.2. Privacy Calculus

Privacy calculus theory assumes that information disclosure is a strategic trade-off between perceived benefits and perceived risks (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Individuals are willing to disclose data when benefits are assessed to outweigh risks, whereas disclosure intention decreases when risks dominate the benefit-risk trade-off (Bojić et al., 2022). In this study, perceived personalization is positioned as an antecedent that simultaneously activates both dimensions of the privacy calculus, which subsequently shape users' willingness to disclose personal data.

2.1.3. Information Asymmetry Theory

Information asymmetry theory describes market contexts where one party possesses superior information over another (Akerlof, 1970). In digital environments like CBRS, an imbalance exists as platforms hold greater information regarding data collection and personalization. Transparency is expected to mitigate this asymmetry by informing users of system operations, thereby reducing uncertainty while heightening trust. In this study, information asymmetry serves as the theoretical basis for the moderating role of transparency.

2.2. The relationship between perceived personalization and privacy calculus

Drawing on the privacy calculus framework and the personalization-privacy paradox, the authors develop hypotheses explaining how perceived personalization influences perceived benefits and perceived risks and how these perceptions affect users' willingness to disclose personal data. Grounded in information asymmetry theory, two additional hypotheses H5a and H5b are formulated to examine the moderating role of transparency in recommendations.

According to privacy calculus theory, individuals' decisions to disclose personal information are the result of a tradeoff between expected benefits and risks (Dinev & Hart, 2006; Xu et al., 2008). This mechanism suggests that users engage in a mental process, weighing positive outcomes against negative consequences before making decision of data disclosure (Laufer & Wolfe, 1977).

Within CBRS, perceived personalization, which refers to how the user subjectively evaluates the relevance and individual fit of recommended content, is expected to activate the benefit dimension of privacy calculus. Personalization enhances relevance, decision quality, and satisfaction. When users perceive that recommended content closely matches their preferences, they recognize tangible benefits of convenience and efficiency (Li & Karahanna, 2015; Tam & Ho, 2006). Drawing on privacy calculus theory and prior literature, users who perceive higher levels of personalization will recognize greater benefits from their engagement with the system, as the relevance and fit of recommendations provide visible value that justifies data disclosure. Therefore:

H1: Perceived personalization positively influences perceived benefits.

While personalization generates benefits, it also activates the risk dimension of privacy calculus through personalization-privacy paradox (Awad & Krishnan, 2006). On the risk side, the same mechanism that enables personalization, specifically extensive data collection and profiling, can make users more conscious of monitoring and loss of control over their personal data (N. Malhotra et al., 2004; Okazaki et al., 2013). As users perceive higher levels of personalization, they become more aware of the data misuse, which in turn heightens their expectations of negative consequences from data sharing. Within the privacy calculus framework, perceived risks is an expression of these concerns by the users under expectations of negative consequences from data disclosure (Dinev & Hart, 2006).

Therefore:

H2: Perceived personalization positively influences perceived risks.

2.3. The relationship between privacy calculus and willingness to disclose data

The privacy calculus theory suggests that the disclosure decision is affected more by perceived benefits in comparison to the perceived risks (Dinev & Hart, 2006). In CBRS contexts, willingness to disclose personal data, including demographic information, location data, device identifiers, and usage patterns, represents users' behavioral intention to share information in exchange for personalized services (Phelps et al., 2000; Sheng et al., 2008).

In line with earlier studies, perceived benefits have a positive influence on disclosure intentions because users are more inclined to provide personal information when they believe that it will provide them with significant returns, even when privacy may be lost (Dinev & Hart, 2006; Krasnova et al., 2010). The enhanced relevance of recommendations is a reason to further allow disclosure of personal information. Thus:

H3: Perceived benefits positively influence willingness to disclose data.

Conversely, the privacy calculus framework also states that intention to disclose personal information is minimized by misuse, unauthorized access, or loss of control (N. Malhotra et al., 2004; Xu et al., 2008). When users perceive higher risks associated with data disclosure, their willingness to share information decreases accordingly. Therefore:

H4: Perceived risks negatively influence willingness to disclose data.

2.4. The Moderating Role of Transparency

Information asymmetry theory posits that digital platforms possess superior knowledge of data practices and algorithmic processes compared to users, creating an informational imbalance (Akerlof, 1970; Pavlou et al., 2007). Transparency functions as a signaling mechanism that reduces this asymmetry by providing credible information about how personalization is generated and how user data are utilized (Awad & Krishnan, 2006; Spence, 1973).

In the privacy calculus, transparency is likely to reestablish the benefit-risk decisions of the users, making the algorithms more understandable and their systems more comprehensible. Previous studies show that perceived quality, usefulness, satisfaction, and intention to use recommendation systems are enhanced by transparency (Herlocker et al., 2004; Knijnenburg et al., 2012; Tintarev & Masthoff, 2007). By making the personalization process understandable and trustworthy, transparency is expected to amplify the positive effect of perceived personalization on perceived benefits. That is, when users understand how their data is collected, they may appreciate the value received from data disclosure, therefore strengthening the personalization-benefit relationship. Accordingly:

H5a: Transparency positively moderates the relationship between perceived personalization and perceived benefits.

Regarding perceived risks, transparency may exert a more complex influence. On one hand, transparency reduces uncertainty and enhances perceived control, thereby mitigating risk perceptions (Culnan & Armstrong, 1999; Metzger, 2007). On the other hand, by revealing the extent of data collection and algorithmic profiling, transparency may heighten users' awareness of potential vulnerability, potentially amplifying perceived risks (Eiband et al., 2018). In the context of personalization, when users are aware of how their data is being used, they may develop more realistic appraisals of privacy risks, reducing the extent to which personalization automatically translates into heightened risk perceptions.

Thus:

H5b: Transparency negatively moderates the relationship between perceived personalization and perceived risks.

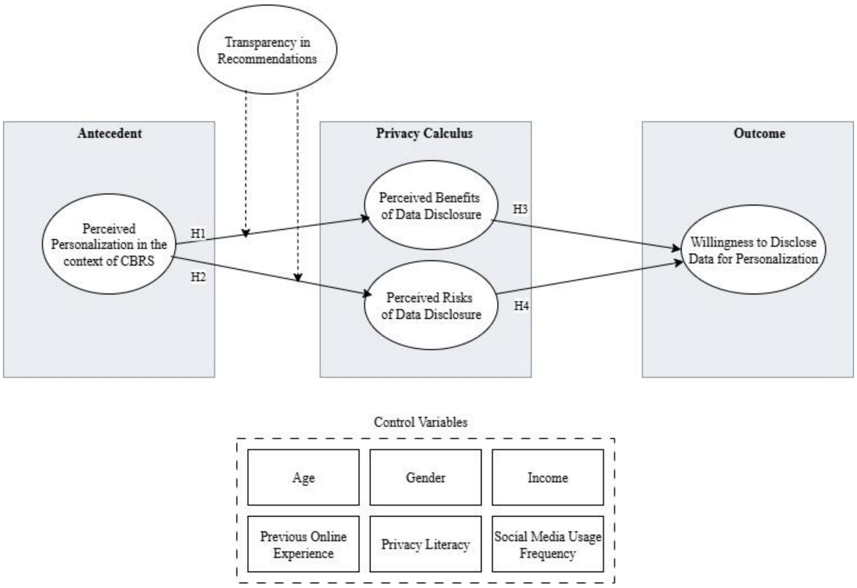

Figure 1: Research Model

Source: Authors' proposal (2026)

3. Methodology

3.1. Data Collection

Data collection was proceeded by the use of Google Forms for six weeks. The final sample was collected using a non-probability purposive sampling technique, consisting of individuals who had prior experience with social media and personalization features. The research team also monitored the age group distribution in reference to the distribution of Internet users during the data collection process to ensure relative age diversity, without imposing fixed quotas for each group.

Following (J. Hair et al., 2021), the minimum sample size for PLS-SEM was estimated using the inverse square root method (Kock & Hadaya, 2018). The minimum path coefficient of the model in previous studies (Kim et al., 2019; Xu et al., 2011; Zhou et al., 2023) was $\beta = 0.2$, and the study adopted a more conservative threshold by assuming a minimum detectable path coefficient of $\beta = 0.15$. The required minimum sample size calculated is, therefore, approximately 275 with $\alpha = 0.05$ and statistical power of 0.80.

The data cleaning process followed the recommendations of (Curran, 2016) for detecting invalid responses in survey data. Responses that failed the attention check question were removed from the dataset. Subsequently, long-string analysis was conducted to identify careless responses, defined as cases in which respondents selected the same option for more than half of the items. A final sample of n = 287, exceeding the recommended threshold, was then used for further analysis.

3.2. Questionaire Design

All constructs in the research model were measured using multi-item scales adapted from prior studies and adjusted to fit the context of the CBRS. Perceived personalization was measured with four items adapted from (Shin, 2020) and (Xu et al., 2011). Transparency was measured with three items adopted from (Shin, 2020). Perceived Benefits was measured using four items based on (McKee et al., 2024). Perceived Risks was measured with six items adapted from (N. K. Malhotra et al., 2004), (Kim et al., 2019). Willingness to Disclose was measured with five items adapted from (Cloarec et al., 2024) and (Jabbar et al., 2023).

All items were measured using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree. The questionnaire was structured into three sections. The questionnaire for the study was divided into three sections: screening questions, demographic and general information, and items measuring core constructs. A pilot test with 30 respondents was conducted to evaluate the clarity and wording of the questionnaire before the main data collection. Several items based on the feedbacks from the pilot test were then slightly revised to improve clarity and readability.

3.3. Data Analysis

After data coding and cleaning, the dataset was analyzed using PLS-SEM with SmartPLS 3.0. The measurement model was assessed following the confirmatory composite analysis procedure recommended by Hair et al. (2022). As all constructs were specified as reflective, reliability and validity were evaluated through indicator loadings, composite reliability, average variance extracted, and discriminant validity using the HTMT criterion with bootstrapping 5,000 resamples.

The structural model was evaluated by examining collinearity, path coefficients, and their significance using bootstrapping with 5,000 resamples. Model explanatory power was assessed using R^2, while effect sizes and predictive relevance were also examined. Mediation effects were tested using bootstrapped specific indirect effects and bias-corrected confidence intervals. Moderation was analyzed using the two-stage approach in PLS-SEM, with mean-centered latent variable scores used to create interaction terms. Conditional indirect effects were examined to assess moderated mediation using the index of moderated mediation.

Control variables including age, gender, income, privacy literacy, social media usage frequency, and prior online experience were included to enhance model robustness.

4. Results and Discussion

The final sample consisted of 287 respondents who have some experience with CBRS. Regarding age distribution, the 18-to-24-year-old shares the largest proportion of 30%, followed by the group of 25-34 years old (26.5%). 35-44, 45-54, and 55+ groups remain 21.2%, 15% and 7.3% consecutively. In terms of gender distribution, the gender sample is relatively balanced with 56.1% females and 43.9% males. Monthly income distribution experience the highest diversity with 29.9% respondents earning under 5,000,000 VND per month salary, followed 27.5% respondents with 10,000,0001-20,000,000 VND in income salary. At the same time, 19.9% of respondents reported with 5,000,001-10,000,000 VND, 13.6% earned between 20,000,001-30,000,000 VND, and 9.1% earned over 30,000,000 VND. Regarding prior online experience, the majority had somewhat experience (43.2%) or extensive experience (34.8%). The remaining parts, constituted of 22% reported limited prior experience with CBRS. In terms of privacy literacy, nearly 90% of the sample reported moderate to high levels of privacy knowledge, with 43.9% reported moderate levels, followed by 32.4% high and 13.6% very high levels. In terms of social media usage, more than two-third of the sample reported spending more than two to more than four hours daily on social media platforms, indicating the high level of social media engagement. The diversity in age, gender income, prior online experience, privacy literacy, and social media usage provides variation for statistical analysis.

4.1. Testing measurement model

The reflective measurement model was evaluated for indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Regarding indicator reliability, most outer loadings exceeded the recommended threshold of 0.70. Three indicators (PP2, PR1 and PR5) did not meet the recommended criteria. Specifically, PR5 exhibited a loading below 0.40 and was therefore removed. Following the guidelines suggested by J. F. Hair et al. (2021) for the two items (PP2 and PR1) with a loading between 0.40 and 0.70, these items were not retained as their removal led to an increase in the AVE of the constructs.

Internal consistency reliability was established as composite reliability values ranged between 0.70 and 0.95, meeting the recommended thresholds. Convergent validity was supported since all AVE values exceeded 0.50. Discriminant validity was assessed using the HTMT criterion. All HTMT values were below the conservative threshold of 0.85, confirming adequate discriminant validity. Overall, the measurement model demonstrates satisfactory reliability and validity.

Table 1: Indicator Loadings, Reliability, and Convergent Validity

Construct	Item	Outer Loading	Composite reliability	AVE
PP	PP1	0.828	0.732	0.646
	PP2	0.652		
	PP3	0.817		
	PP4	0.775		
PB	PB1	0.882	0.836	0.673

Construct	Item	Outer Loading	Composite reliability	AVE
	PB2	0.776		
	PB3	0.875		
	PB4	0.742		
PR	PR1	0.685	0.866	0.712
	PR2	0.870		
	PR3	0.870		
	PR4	0.789		
	PR5	0.371		
	PR6	0.808		
TR	TR1	0.751	0.768	0.679
	TR2	0.885		
	TR3	0.831		
WTD	WTD1	0.803	0.852	0.625
	WTD2	0.816		
	WTD3	0.754		
	WTD4	0.803		
	WTD5	0.776		

Note. PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Data collected from 287 respondents (2026)

Table 2: Heterotrait-Monotrait Ratio (HTMT) Matrix

	PP	PB	PR	TR	WTD
PP	-				
PB	0.542	-			
PR	0.227	0.252	-		
TR	0.237	0.584	0.143	-	
WTD	0.290	0.410	0.159	0.242	-

Note. PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Data collected from 287 respondents (2026)

4.2. Testing structural model

After conducting the reliability test and concluding that the model is reasonably fit, structural equation modeling was employed to examine whether the hypotheses are true or not. The results of the test are demonstrated as follows:

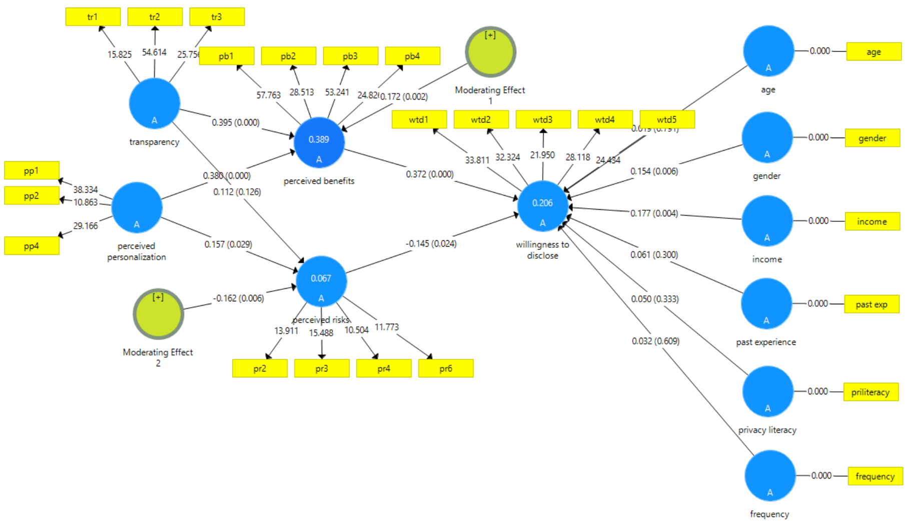

Figure 2: SEM Results

Source: Data collected from 287 respondents (2026)

The structural model was evaluated using Bias-Corrected and Accelerated (BCa) bootstrapping with 5,000 resamples and a two-tailed significance level of 5%. The moderating effects were examined using the two-stage approach as it is preferable when the measurement model is reflective (Hair et al., 2022). Collinearity diagnostics showed that all inner VIF values were below the recommended threshold of 3.3, indicating no multicollinearity concerns.

Table 3: Structural Equation Modeling Results

Hypothesis	Path	Original Sample (O)	Sample Mean (M)	STDEV	T Statistic	P Values	Result
H1	PP→ PB	0.380	0.383	0.051	7.494	0.000***	Supported
H2	PP → PR	0.157	0.161	0.072	2.182	0.029**	Supported
H3	PB→WTD	0.372	0.373	0.054	6.871	0.000***	Supported
H4	PR → WTD	-0.145	-0.149	0.064	2.263	0.024**	Supported
H5a	Moderation 1	0.172	0.167	0.055	3.122	0.002**	Supported
H5b	Moderation 2	-0.162	-0.157	0.059	2.734	0.006**	Supported

Note. ***: P<0.001; **: P<0.05; *: P<0.1; PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Moderation 1: TR moderates the path of PP → PB; Moderation 2: TR moderates the path of PP → PR; Data collected from 287 respondents (2026)

According to Table 3, all six hypothesized relationships are statistically significant. Specifically, perceived personalization has a positive and significant effect on perceived benefits and perceived risks, supporting H1 and H2. In addition, perceived benefits positively influence willingness to disclose personal information while perceived risks negatively influence willingness to disclose. Therefore, H3 and H4 are also supported.

Regarding the moderating effects, the results show that both interactions between transparency and perceived personalization on perceived benefits and perceived risks are statistically significant. These findings indicate that transparency does significantly influence the strength of the relationships between perceived personalization and both perceived benefits and perceived risks. Therefore, H5a and H5b are supported.

Table 4: Coefficient of Determination

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
PB	0.389	0.400	0.043	8.987	0.000***
PR	0.067	0.082	0.037	1.801	0.072*
WTD	0.206	0.230	0.045	4.619	0.000***

Note. ***: P<0.001; **: P<0.05; *: P<0.1; PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Data collected from 287 respondents (2026)

Regarding the explanatory power of the model, the coefficient of determination R^2 shows that perceived personalization explains 38.9% of the variance in perceived benefits, indicating moderate explanatory power. In contrast, the model explains only 6.7% of the variance in perceived risks, suggesting weak explanatory ability for this construct. For willingness to disclose, the model accounts for 20.6% of the variance, which is weak explanatory power according to Hair et al. (2011).

Table 5: Effect size

Path	Path coefficient	f^2	Interpretation
PP → PB	0.380	0.227	Medium effect
PP → PR	0.157	0.025	Small effect
PB→WTD	0.372	0.141	Small effect
PR→WTD	-0.145	0.022	Small effect
Moderation 1	0.172	0.045	Small effect
Moderation 2	-0.162	0.027	Small effect

Note. ***: P<0.001; **: P<0.05; *: P<0.1; PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Moderation 1: TR moderates the path of PP → PB; Moderation 2: TR moderates the path of PP → PR; Data collected from 287 respondents (2026)

Following the guidelines of Hair et al. (2022), the results show that perceived personalization has a medium effect on perceived benefits, suggesting that perceived personalization is a substantial predictor of pereived benefits in the model. In contrast, all other relationships exhibit small effect sizes. Additionally, the moderating effects of transparency on the relationships between perceived personalization and perceived benefits and between perceived personalization and perceived risks are also small.

Table 6: Predictive Relevance

	SSO	**SSE**	**Q^2**
PB	804	586.329	0.276
PR	1206	1196.561	0.040
WTD	1005	881.613	0.109

Note. ***: P<0.001; **: P<0.05; *: P<0.1; PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Data collected from 287 respondents (2026)

The results show that perceived benefits has a Q^2 value of 0.276, indicating moderate predictive relevance. Willingness to disclose achieves a Q^2 value of 0.109, suggesting small predictive relevance. In contrast, perceived risks has a value of 0.040 which is close to 0 and shows negligible predictive relevance. All other exogenous constructs show values equal to 0 because predictive relevance is only assessed for endogenous constructs.

4.3. Discussion

The main objective of this paper is to examine the influence of perceived personalization on users' willingness to disclose personal data, with transparency being incorporated as a moderator. The study extends the privacy calculus scope, therefore providing significant insights for both social media users and platform developers.

Aligning with Awad and Krishnan (2006) research on the benefit-risk trade-off in data disclosure, the results further confirm that perceived personalization increases perceived benefits and the effect of this mechanism is stronger than its impact on perceived risks. Perceived benefits, at the same time, significantly determine the willingness to disclose personal data. On platforms such as TikTok, YouTube, and Facebook Reels, people continuously disclose behavioral data such as likes, watch history, and location. Despite being aware that such platforms utilize personal data, many users still accept the situation as long as the personalization features provide relevant advertisements and videos. This finding reinforces the statement that individuals tend to appreciate visible benefits over abstract privacy risks in the contexts of personalization. However, different from Awad and Krishnan (2006) the present study reveals the statistically significant results of perceived risks in shaping users' perceptions, despite the visible benefits perceived.

This finding is, otherwise, consistent with Xu et al. (2011) study on the personalization-privacy paradox, which emphasizes the role of perceived control in location-aware marketing. By comparing between covert and overt data disclosure conditions, Xu et al. (2011) pointed out that perceived control acts as an moderator in users' benefit-risk assessment. Similarly, this study on the contexts of CBRS, has further confirmed the dual mechanisms of transparency: while transparency heightens the relationship between personalization and perceived benfits, it also weakens the tension between personalization and privacy risks.

The moderating role of transparency in recommendations is also the most critical finding of this study. The results show that transparency significantly moderates both the personalization-benefit relationship and personalization-risk relationship, proving that transparency does not simply act as a benefit amplifier but also as a risk reduction.

These findings align with Tintarev and Masthoff (2012) study on explainability in recommendation systems, which indicates that explainability enhances user assessment through two mechanisms: perceived benefits and perceived risks. Our study, building upon this foundation, pointed out that this mechanism is also a moderator that reshapes the way personalization influences user perceptions of risks and benefits. When users understand why specific content is recommended in their social feeds, the value of personalization features becomes more salient. At the same time, transparency enables users to validate the recommendation process and ensures that their data are used in accordance with established rules, thereby reducing privacy concerns (Xu et al., 2011). TikTok is now incorporating the feature "Why am I seeing this" to explain why specific content is being recommended to users. Google similarly introduces Ads Transparency which allows users to adjust their personal data used for personalized advertisements. Such mechanisms make the recommendation process more transparent, thereby heightening trust among individuals while reducing privacy concerns of data misuse.

Overall, this study contributes to the literature by demonstrating that personalization operates as a dual mechanism of benefits and risks, with privacy risks remaining relevant in recommendation systems, and that transparency functions as both a benefit amplifier and risk intensifier. These findings broaden the application of privacy calculus theory to recommendation system environments.

5. Conclusion and Implications

5.1. Conclusion and limitations

The research aims to investigate the influence of perceived personalization on willingness to disclose personal information through two intermediate mechanisms of perceived benefits and perceived risk in the context of the CBRS. Furthermore, the assessment of the moderating role of transparency in these relationships was also a focus of this study. With these objectives, the results are able to provide empirical support for all hypothesized relationships. Particularly, perceived personalization increases both perceived benefit and perceived risk, and both constructs significantly influence willingness to disclose information in opposite directions.

Importantly, transparency plays a significant moderating role in the examined model. When transparency is at a high level, the positive influence of perceived personalization on perceived benefit is amplified, while the influence on perceived risk is weakened. This demonstrates that level of transparency is an important factor that affects how users interpret personalization practices.

This study contributes to the literature in two ways. First, it provides empirical support for the privacy calculus framework by validating the relationships among perceived personalization, perceived benefits, perceived risks, and willingness to disclose in the context of the CBRS. Second, the study extends the existing model by examining the moderating role of transparency, highlighting its importance in shaping how users interpret personalization practices.

From a practical perspective, the findings provide useful insights for both social media users and platform developers in managing the balance between the benefits and privacy risks associated with personalization practices. Platforms can enhance perceived benefits while mitigating perceived risks by improving transparency in how personal data is collected and utilized, thereby encouraging users to disclose personal information more willingly.

As for limitations, the study employed purposive sampling, which may result in an unrepresentative sample. Another limitation concerns the limited variation of perceived risk, which may result from survey design or data collection method. This restriction in variation can reduce the ability to detect the statistically significant effects of perceived risk. The data was collected through a self-assessed online survey on Google Form, therefore, may bear the risks of common method bias and self-report bias. Furthermore, the study stops at measuring the intention of disclosing data, which can lead to an intention-behavior gap.

Therefore, for a more rigorous and generalizable examination, future studies can expand the sample size, employ probability sampling methods, and refine the measurement design to collect greater variability in key constructs. The robustness of the findings can also be enhanced by applying multiple data collection methods. Future studies may also extend the model by exploring other potential moderating variables to have a better understanding of the proposed relationship.

5.2. Implications

The study results offer practical insights for both social media users and platform developers in balancing between benefits and risks derived from personalization features.

An asymmetric influence of perceived personalization on the privacy calculus was demonstrated in the results: the effect on perceived benefit is 2.5 times higher than that on perceived risk. This indicates that users are likely to view personalization features as benefits rather than privacy risks. Users, however, need to perceive personalization as a dual mechanism, increasing both user experience and privacy concerns. For social media users, interaction with personalization features is hence implied as a non-neutral process, as it contributes to enhancing user experience and heightening privacy concerns at the same time

The results also reveal that data disclosure on social media is a complex process. Specifically, the benefits from personalization increase willingness to disclose data, and perceived risks show an opposing effect. This suggests that gains act as the primary driver of data disclosure, while privacy concerns can be seen as the barrier. Therefore, a more deliberate evaluation process may help users make more informed decisions on disclosing information.

For platform developers, the findings suggest priortizing investments that enhance the quality of personalization features. Improvements that strengthen users' perceived value are more likely to translate into increased engagement and data disclosure than initiatives focused solely on risk communication. Therefore, platforms should not only rely on warning users about risks, but also clearly communicate the practical benefits of personalizations while ensuring strong privacy safeguards.

The research also demonstrates that transparency plays a complex role, significantly moderating the relationships between personalization and both perceived benefits and perceived risks. This means that when platforms designed clearly explain their data practices, the perceived personalization-benefit relationship is strengthened while the personalization-risk relationship is weakened. In other words, transparency in recommendations makes users more attentive to the advantages of personalization features, while reduce privacy concerns about data intrusions. Therefore, transparency should not be treated as a simple compliance requirement. Platforms should present transparency in a user-focused method by showing how their data is used to create values while also explaining how risks are effectively managed. By doing so, platforms can enhance perceived benefits while mitigating users' privacy concerns.

References

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.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism*. *The Quarterly Journal of Economics*, *84*(3), 488-500.

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13-28.

Bojić, L., Bulatović, A., & Žikić, S. (2022). The Scary Black Box: AI Driven Recommender Algorithms as The Most Powerful Social Force. *Etnoantropološki problemi / Issues in Ethnology and Anthropology*, *17*(2), 719–744.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2), 181-202.

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2021). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, *39*, 647-661.

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media. *Psychology & Marketing*, *41*, 1574-1596.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Curran, P. G. (2016). Methods for the detection of carelessly invalid responses in survey data. *Journal of Experimental Social Psychology*, *66*, 4-19.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Info. Sys. Research*, *17*(1), 61–80.

Eiband, M., Schneider, H., Bilandzic, M., Fazekas-Con, J., Haug, M., & Hussmann, H. (2018). *Bringing Transparency Design into Practice* Proceedings of the 23rd International Conference on Intelligent User Interfaces, Tokyo, Japan.

Hair, J., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*.

Hair, J., Hult, G. T. M., Ringle, C., Sarstedt, M., Danks, N., & Ray, S. (2021). *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A workbook*.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152.

Herlocker, J., Terveen, L., Lui, J. C. s., & Riedl, T. (2004). Evaluating collaborative filtering recommender systems. *ACM Transactions on Information Systems*, *22*, 5-53.

Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance*, *64*, 101826.

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281.

Knijnenburg, B. P., Willemsen, M. C., Gantner, Z., Soncu, H., & Newell, C. (2012). Explaining the user experience of recommender systems. *User Modeling and User-Adapted Interaction*, *22*(4), 441-504.

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227–261.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, *25*(2), 109-125.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22-42.

Li, S., & Karahanna, E. (2015). Online Recommendation Systems in a B2C E-Commerce Context: A Review and Future Directions. *Journal of the Association for Information Systems*, *16*, 72-107.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*, 336-355.

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.

McKee, K. M., Dahl, A. J., & Peltier, J. W. (2024). Gen Z's personalization paradoxes: A privacy calculus examination of digital personalization and brand behaviors. *Journal of Consumer Behaviour*, *23*(2), 405-422.

Metzger, M. J. (2007). Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, *58*(13), 2078-2091.

Okazaki, S., Li, H., & Hirose, M. (2013). Consumer Privacy Concerns and Preference for Degree of Regulatory Control. *Journal of Advertising*, *38*, 63-77.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal–Agent Perspective1. *Management Information Systems Quarterly*, *31*(1), 105-136.

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.

Sheng, H., Nah, F., & Siau, K. (2008). An Experimental Study on Ubiquitous commerce Adoption: Impact of Personalization and Privacy Concerns. *J. AIS*, *9*.

Shin, D. (2020). User Perceptions of Algorithmic Decisions in the Personalized AI System:Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability. *Journal of Broadcasting & Electronic Media*, *64*, 1-25.

Spence, M. (1973). Job Market Signaling*. *The Quarterly Journal of Economics*, *87*(3), 355-374.

Statista. (2025). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028*. Available at: www.statista.com

Strycharz, J., van Noort, G., Helberger, N., & Smit, E. (2019). Contrasting perspectives – practitioner's viewpoint on personalised marketing communication. *European Journal of Marketing*, *53*(4), 635-660.

Tam, K., & Ho, S. (2006). Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, *30*, 865-890.

Tintarev, N., & Masthoff, J. (2007, 17-20 April 2007). A Survey of Explanations in Recommender Systems. 2007 IEEE 23rd International Conference on Data Engineering Workshop,

Tintarev, N., & Masthoff, J. (2012). Evaluating the effectiveness of explanations for recommender systems: Methodological issues and empirical studies on the impact of personalization. *User Modeling and User-Adapted Interaction*, *22*(4), 399-439.

Trūata. (2021, 09.01.2025). *Global Consumer State of Mind Report 2021*. Trūata. Retrieved 7/9/2025 from www.content.truata.com

We are Social. (2025, 09.01.2025). *Digital 2025 Global Overview Report*. Retrieved 7/9/2025 from www.wearesocial.com

Xu, H., Dinev, T., Smith, H., & Hart, P. (2008). *Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View*.

Xu, H., Luo, X., Carroll, J., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*, 42-52.

Zhang, Q., Lu, J., & Jin, Y. (2021). Artificial intelligence in recommender systems. *Complex & Intelligent Systems*, *7*(1), 439-457.

Zhou, H., Xiong, F., & Chen, H. (2023). A Comprehensive Survey of Recommender Systems Based on Deep Learning. *Applied Sciences*, *13*(20). Retrieved 5/10/2025, from

Table A. Measurement Scales

Construct	Coding	Question Wording	Sources
PP- Perceived Personalization			
PP	PP1	I think that the recommended contents by CBRS reflect my preferences.	(Shin, 2020)
	PP2	It seems that the CBRS is customized to me.	
	PP3	The CBRS can provide me with personalized content tailored to my activity context.	(Xu et al., 2011)
	PP4	The CBRS can provide me with the kind of content that I might like	
TR - Transparency in Recommendations			
TR	TR1	I think that the evaluation and the criteria of CBRS used for personalization are publicly released and understandable to people. (Understandability)	(Shin, 2020)
	TR2	Any outputs produced by a CBRS are explainable to the people affected by those outputs. (Explainability)	
	TR3	CBRS lets people know how well their internal processes can be understood from their external outputs. (Observability)	
PB - Perceived Benefits			

PB	PB1	Using personalization features from the CBRS improves my online experience	(McKee et al., 2024)
	PB2	Personalized content by the CBRS makes my online searches more effective	
	PB3	Personalization from the CBRS enables me to find content I need more easily on social media.	
	PB4	Continuing to use personalization features from the CBRS would be useful when browsing online	
PR - Perceived Risks			
PR	PR1	In general, it would be risky to give the information to the CBRS	(N. K. Malhotra et al., 2004)
	PR2	I believe there is the risk due to the possibility that personal information tracked by CBRS could be sold to third parties	(Kim et al., 2019)
	PR3	I believe there is the risk due to the possibility that personal information tracked by CBRS could be misused	
	PR4	I believe there is the risk due to the possibility that personal information tracked by CBRS could be made available to unknown individuals or companies without your knowledge	
	PR5	I believe there is the risk due to the possibility that personal information tracked by CBRS could be made available to governmental agencies	

	PR6	I believe there is the risk due to the possibility that personal information tracked by CBRS could be jeopardized by hacking activities	
WTD - Willingness to Disclose Data			
Willingness in specific context	WTD1	I intend to disclose my personal information if the CBRS recommends content based on my purchasing behavior and my search history performed on its website	(Cloarec et al., 2024)
	WTD2	I intend to disclose my personal information if the CBRS recommends content based on the preferences of my SNS friends	
	WTD3	I intend to disclose my personal information if the CBRS recommends content based on my geolocation once activated on my smartphone, my computer or my tablet	
General willingness	WTD4	I am willing to provide my personal information when asked by the CBRS	(Jabbar et al., 2023)
	WTD5	I am willing to be truthful in revealing my personal information to the CBRS	

Note. PP: Perceived Personalization; PB: Perceived Benefits; PR: Perceived Risks; WTD: Willingness to Disclose; TR: Transparency; Author's proposal (2026)