



THE PERSONALIZATION–PRIVACY PARADOX IN SOCIAL COMMERCE: WHY PRIVACY CONCERN DOES NOT DETER WILLINGNESS TO BE PROFILED ON TIKTOK SHOP

To Anh Tho^{1*}, Pham Le Quynh Anh¹, Nguyen Thien Long¹,
Quan Minh Quan¹, Nguyen Minh Thu¹

¹University of Finance - Marketing, Vietnam

ARTICLE INFO	ABSTRACT
DOI: 10.52932/jfmr.v17i1enes.1333 <i>Received:</i> April 07, 2026 <i>Accepted:</i> June 23, 2026 <i>Published:</i> August 08, 2026 Keywords: Customer trust, Online personalization, Privacy concern, TikTok shop, Willingness to be profiled Article classification: Research paper JEL codes: M30, M31, M37	Purpose – This study examines how online personalization, technical protection, and privacy awareness are associated with privacy concern, customer trust, and willingness to be profiled online for personalization among TikTok Shop users in Vietnam. Integrating Privacy Calculus Theory (PCT) and the Stimulus–Organism–Response (SOR) framework, the study explores how personalization-related stimuli shape users’ privacy evaluations and acceptance of profiling in the context of short-video social commerce. Design/methodology/approach – Data from 300 TikTok Shop users were analyzed using PLS-SEM in SmartPLS 4.0 with 5,000 bootstrap resamples. Findings – Online personalization increased privacy concern, customer trust, and willingness to be profiled. Technical protection strengthened customer trust but did not reduce privacy concern. Contrary to the proposed negative relationship, privacy awareness increased privacy concern, while also strengthening customer trust. Privacy concern was positively related to willingness to be profiled, also contrary to the hypothesized direction. Customer trust was the strongest predictor of profiling acceptance. Originality/value – The study extends the personalization–privacy paradox to TikTok Shop in an emerging market. It shows that personalization can simultaneously increase privacy concern, trust, and profiling acceptance, while customer trust serves as the dominant predictor and mediating mechanism.

*Corresponding author:

Email: totho@ufm.edu.vn

Practical implications – TikTok Shop and similar platforms should strengthen customer trust by clearly communicating data-protection practices, explaining how personal data are used, and providing meaningful consent and user-control options. Personalization should remain valuable without becoming overly intrusive.

Social implications – Greater transparency, informed consent, and user control can support more informed data-sharing decisions and more responsible algorithmic profiling in social commerce.

1. Introduction

The rapid development of digital technologies and social commerce platforms has significantly transformed the way consumers search for information and make purchasing decisions. Among these platforms, TikTok Shop has emerged as a prominent social commerce ecosystem, particularly attracting users in Vietnam through its highly personalized recommendation system. By leveraging algorithm-driven personalization, the platform provides tailored product suggestions that enhance convenience and improve the online shopping experience (Bleier & Eisenbeiss, 2015; Martin & Murphy, 2017). Unlike traditional e-commerce platforms (e.g., Shopee, Lazada) that primarily rely on search-based purchasing behavior, TikTok Shop operates through a short-video, algorithm-driven ecosystem in which product discovery is deeply embedded within entertainment content and personalized recommendations.

However, the increasing reliance on personalization technologies has also raised concerns about the collection and use of personal data. While personalized recommendations can create value for consumers, they often require access to large amounts of user data, raising privacy concerns (Xu et al., 2011; Smith et al., 2011). This tension between the benefits of personalization and the risks related to privacy is widely referred to as the personalization–

privacy paradox, a phenomenon that has attracted growing attention in digital commerce research (Awad & Krishnan, 2006; Chellappa & Sin, 2005). In the context of TikTok Shop, profiling and algorithmic recommendations are not merely supporting marketing tools but central mechanisms that shape users' browsing, entertainment, and purchasing experiences. As a result, users may continue accepting personalization despite experiencing privacy-related concerns.

Previous studies have explored the role of personalization and privacy in shaping consumer behavior in online environments. Research suggests that personalization can improve user engagement and satisfaction, while privacy concerns may discourage individuals from sharing personal data with digital platforms (Xu et al., 2011; Bansal et al., 2010). However, much of the existing literature has focused on traditional e-commerce or social media platforms rather than short-video social commerce environments driven by continuous algorithmic curation. Consequently, traditional privacy trade-off assumptions may not fully explain user behavior in platforms such as TikTok Shop, where personalization is closely integrated with entertainment consumption and platform engagement. Despite these findings, limited research has examined how different privacy-related factors interact to influence

customer trust and users' willingness to share data in social commerce contexts, particularly in emerging markets such as Vietnam (Xu et al., 2011).

To address this gap, the present study investigates the relationships among online personalization, technical protection, privacy awareness, privacy concern, customer trust, and willingness to be profiled online among TikTok Shop users. Specifically, the study examines how stimulus-related factors shape users' internal evaluations of privacy concern and customer trust, and how these evaluations are associated with willingness to accept profiling for personalized services in a social commerce context. By integrating Privacy Calculus Theory (PCT) and the Stimulus – Organism - Response (S-O-R) framework, this study further explores whether traditional privacy assumptions remain applicable in algorithm-driven short-video commerce environments. The study contributes to the literature by extending the personalization-privacy paradox into the context of TikTok Shop and highlighting the dominant role of customer trust in shaping users' acceptance of profiling despite privacy-related concerns.

The remainder of this paper is organized as follows. Section 2 reviews the relevant literature and develops the research hypotheses. Section 3 describes the research methodology. Section 4 presents empirical results and discussion. Finally, Section 5 concludes the study and outlines its implications and limitations.

2. Literature Review

2.1. Privacy Calculus Theory and S-O-R Framework

In digital commerce environments, consumers often face a trade-off between the benefits of personalized services and the risks of disclosing personal information. This phenomenon is commonly explained by

Privacy Calculus Theory (PCT), which suggests that individuals evaluate the perceived benefits and risks before deciding whether to share personal data (Dinev & Hart, 2006; Kezer et al., 2022). When the perceived benefits outweigh the privacy risks, consumers are more willing to disclose their personal information (Kezer et al., 2022).

In addition, the Stimulus-Organism-Response (S-O-R) framework provides a theoretical explanation for how external stimuli influences consumer behavior. In this framework, environmental factors act as stimuli that influence individuals' internal psychological states, which subsequently lead to behavioral responses (Saha & Ali, 2024; Hoang & Dang, 2024). In the context of social commerce, factors such as online personalization, technical protection, and privacy awareness can be considered external stimuli that affect consumers' internal evaluations, particularly privacy concern and customer trust, which ultimately influence their willingness to disclose personal information (Pavlou, 2003; Saha & Ali, 2024).

In this study, Privacy Calculus Theory explains the trade-off between personalization-related benefits and privacy-related risks, while the S-O-R framework provides a process-oriented explanation of how external personalization stimuli influences users' internal psychological evaluations and subsequent behavioral responses. Integrating these two frameworks allows the study to examine not only whether users perceive privacy-related risks and benefits, but also how these evaluations shape willingness to accept profiling in the context of algorithm-driven social commerce.

2.2. TikTok Shop Algorithm and AI-Driven Personalization

General personalization theories explain how tailored recommendations influence consumer trust and privacy concerns, yet TikTok Shop's

algorithm represents a distinctive case in social commerce. Unlike conventional e-commerce platforms such as Amazon or Shopee, which rely on search-based queries and collaborative filtering, TikTok Shop integrates product recommendations directly into TikTok's entertainment ecosystem. Products are embedded within short-form videos and surfaced through the "For You Page," where algorithmic curation is driven by engagement signals such as watch time, likes, shares, and comments.

Systematic reviews emphasize that TikTok's algorithm amplifies marketing effectiveness by merging entertainment with commerce. By embedding products into viral content and influencer-driven trends, TikTok Shop maximizes engagement and conversion, positioning itself as a hybrid between social media and e-commerce (Melgarejo-Espinoza et al., 2025). This approach differs from traditional platforms, where exposure is largely determined by keyword relevance or seller reputation.

Artificial intelligence is central to this process. TikTok employs natural language processing to interpret captions and comments, computer vision to identify products within video frames, and audio recognition to detect trending sounds associated with product promotions. These AI-driven mechanisms enable TikTok Shop to test product-related videos with small user cohorts and expand distribution when engagement is high, thereby shaping consumer preferences dynamically. Evidence from Vietnam further shows that live streaming, video content, and AI recommendations mediated by key opinion consumers (KOCs) significantly enhance TikTok Shop adoption, underscoring the platform's reliance on algorithmic personalization to build trust and purchase intent (Le et al., 2025). These characteristics suggest that traditional privacy trade-off assumptions may operate differently in algorithm-driven short-video commerce environments, where personalization is closely integrated with entertainment consumption,

continuous user engagement, and algorithmic content discovery.

2.3. Technical protection

Technical protection refers to technological mechanisms designed to safeguard users' personal data during online interactions. These mechanisms include encryption technologies, authentication systems, secure servers, and firewall protections that prevent unauthorized access to user information (Kim et al., 2009; Chellappa & Pavlou, 2002). Strong security measures can reduce consumers' perceived privacy risks and increase confidence in digital platforms (Bélanger & Crossler, 2011). Within the privacy calculus perspective, the presence of robust technical protection reduces consumers' privacy concerns because users believe that their personal data will be handled securely. Therefore, the following hypothesis is proposed:

Hypothesis H1: Technical protection negatively influences privacy concern.

In online transactions, trust is essential because consumers cannot directly verify the service provider's intentions or abilities. Technical protection mechanisms act as signals of competence, integrity, and benevolence, which are key dimensions of trust (Kim et al., 2009; Chellappa & Pavlou, 2002; Pavlou, 2003). When customers perceive strong safeguards, their confidence in the platform's ability to securely manage personal information increases, thereby enhancing trust (Bélanger & Crossler, 2011). Thus, the following hypothesis is proposed:

Hypothesis H2: Technical protection positively influences customer trust.

2.4. Privacy awareness

Privacy awareness refers to consumers' understanding of how online platforms collect, process, use, and share their personal information (Sah & Jun, 2024; Smith et al., 2011). From a privacy calculus perspective,

greater privacy awareness may help consumers evaluate data disclosure more rationally by reducing uncertainty about how their information is handled. When users understand why their personal data are collected and how such data support personalized services, they may perceive the data exchange as more predictable, transparent, and manageable. In the context of TikTok Shop, users with higher privacy awareness may therefore experience lower privacy concern because they better understand the platform's data practices. At the same time, this awareness may enhance customer trust by strengthening perceptions of platform transparency, competence, and responsible data management. Thus, the following hypotheses are proposed:

Hypothesis H3: Privacy awareness negatively influences privacy concern.

Hypothesis H4: Privacy awareness positively influences customer trust.

2.5. Online Personalization

Online personalization refers to the practice of tailoring products, services, or digital content to individual consumers based on their preferences, behaviors, and personal data (Xu et al., 2011). Personalized services can improve user experience by providing relevant recommendations and enhancing convenience during online shopping. However, personalization typically requires the collection and analysis of large amounts of personal information, which may raise concerns about privacy and data misuse. As a result, consumers may become more concerned about how their personal data is used. Thus, the following hypothesis is proposed:

Hypothesis H5a: Online personalization positively influences privacy concern.

Despite the potential for privacy concerns, personalized services may simultaneously

foster customer trust when users perceive that the firm understands their needs and provides relevant, convenient, and value-added offerings (Tam & Ho, 2006). Personalization signals that the company invests effort in building long-term relationships with customers, thereby increasing perceived care, satisfaction, and trust (Pappas et al., 2014). Therefore, the following hypothesis is proposed:

Hypothesis H5b: Online personalization positively influences customer trust.

2.6. Privacy concern and willingness to be profiled

Privacy concern refers to individuals' worries about how their personal information is collected, stored, and used by organizations (Smith et al., 2011; Dinev & Hart, 2006). When consumers perceive higher privacy risks, they may become reluctant to disclose personal data or participate in personalized services. Therefore, higher levels of privacy concern may reduce consumers' willingness to allow platforms to collect and analyze their personal data for personalization purposes.

Hypothesis H6: Privacy concern negatively influences willingness to be profiled online for personalization.

2.7. Customer trust and willingness to be profiled

Customer trust refers to consumers' belief that an online platform is reliable, honest, and capable of protecting their interests (Gefen et al., 2003; Pavlou, 2003). Trust plays a critical role in reducing perceived risks and encouraging consumers to engage in online transactions. When consumers trust a platform, they are more willing to share personal information and accept personalized services. Accordingly, the following hypothesis is proposed:

Hypothesis H7: Customer trust positively influences willingness to be profiled online for personalization.

In addition to privacy concern and customer trust, online personalization itself can directly motivate consumers' willingness to be profiled. When users perceive personalized services as relevant and valuable, they are more inclined to share personal data despite privacy risks (Awad & Krishnan, 2006; Xu et al., 2011). Within the privacy calculus framework, personalization represents a perceived benefit that encourages

disclosure (Pavlou, 2003; Dinev & Hart, 2006). Studies further suggest that personalized experiences may foster perceptions of reciprocity, where consumers feel that data sharing is justified by the value received (Pappas et al., 2014).

Hypothesis H8: Online personalization positively influences willingness to be profiled online for personalization.

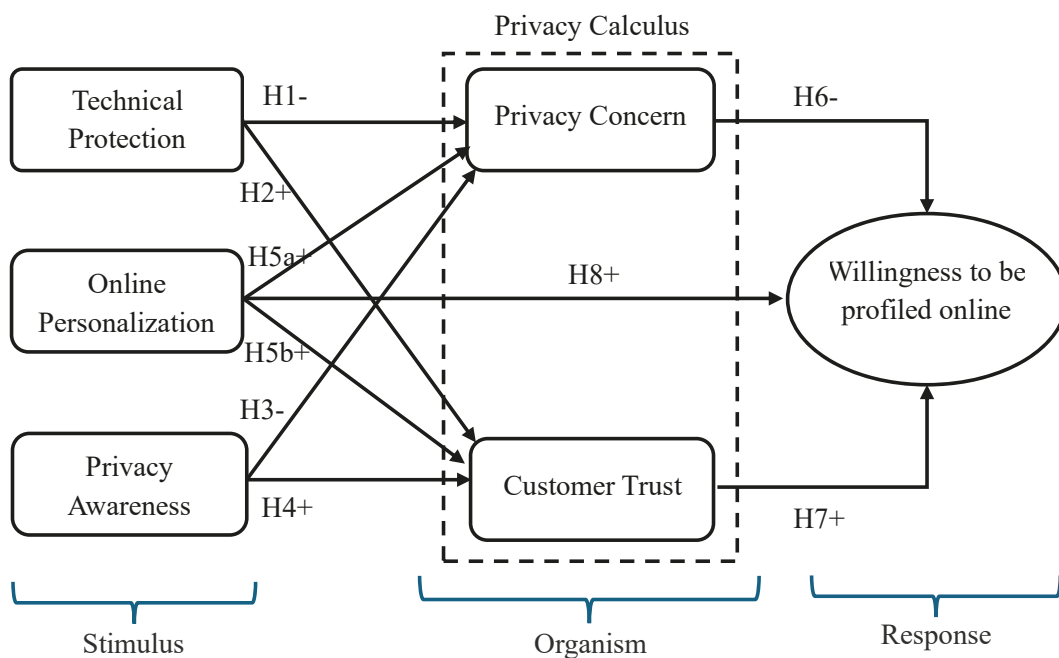


Figure 1. Proposed Research Model

3. Methodology

A quantitative research approach was employed to examine the personalization–privacy paradox in social commerce, particularly among TikTok Shop users in Vietnam. Data were collected through an online survey using a structured questionnaire based on measurement scales adapted from previous studies related to online privacy, personalization, and trust (As shown in Appendix A). The questionnaire was translated into Vietnamese to ensure respondents' understanding and was distributed via Google Forms, enabling convenient participation while maintaining respondent

anonymity. Data collection was conducted between July and August 2025. Participation was voluntary, and respondents were informed that their responses would be used solely for academic research purposes.

A non-probability convenience sampling method was employed to collect responses through online communities and social media groups. A total of 380 responses were initially obtained. After removing incomplete or inconsistent responses during the data screening, 300 valid responses were retained for further analysis. This sample size was considered appropriate for the analytical method applied in

this study. The final sample size was considered adequate for PLS-SEM analysis and consistent with recommendations for structural equation modeling involving multiple latent constructs.

The questionnaire was structured into two main sections. The first section collected demographic information, including respondents' gender, age, education level, and income. The second section measured the key constructs in the research model, including online personalization, technical protection, privacy awareness, privacy concern, customer trust, and willingness to be profiled online for personalization. All measurement items were assessed using a five-point Likert scale ranging from "strongly disagree" to "strongly agree".

To analyze the collected data and test the proposed hypotheses, the study employed Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4.0 software. This analytical technique is widely used in marketing and information systems research because it can effectively analyze complex models involving multiple latent constructs and relationships. The analysis followed a two-step procedure. *First*, the measurement model was evaluated to assess the reliability and validity of the constructs, including internal consistency reliability (Cronbach's alpha and composite reliability), convergent validity using Average Variance Extracted (AVE), and discriminant validity using the Heterotrait–Monotrait ratio (HTMT). *Second*, the structural model was assessed to test the proposed hypotheses by examining path coefficients and statistical significance through a bootstrapping procedure with 5,000 resamples. This approach allows the study to evaluate the relationships among personalization, technical protection, privacy awareness, privacy concern, customer trust, and users' willingness to disclose personal information for personalized services.

Data was collected through an online survey of 300 TikTok Shop users in Vietnam. While the sample is concentrated within the 18-24 age group (71.67%), this demographic closely reflects the dominant user segment of TikTok Shop and short-video social commerce platforms in Vietnam. To ensure methodological rigor, Harman's Single Factor Test was conducted to assess Common Method Bias (CMB), indicating that no single factor accounted for more than 50% of the variance (as shown in Appendix B). In addition, R^2 , f^2 , and Q^2 values were assessed to evaluate the model's explanatory power, effect sizes, and predictive relevance.

4. Results and discussion

4.1. Descriptive statistics

Appendix 2 (*see Appendix 2 online*) presents the demographic profile of the sample based on 300 valid responses collected in July 2025 from users of TikTok Shop in Vietnam. Of the participants, 188 (62.7%) are female, and 112 (37.3%) are male. The largest age group comprises individuals aged 18-24 ($n = 215$; 71.67%), followed by 25-34 ($n = 60$; 20.0%). In terms of education, most respondents hold a Bachelor's degree ($n = 210$; 70.0%), and most identify as students ($n = 207$; 69.0%). The dominant income band is under 5 million VND ($n = 158$; 52.7%), while the over 30 million VND category accounts for the smallest percentage. The demographic profile suggests that the sample largely reflects the dominant user segment of TikTok Shop in Vietnam, particularly younger users who are highly engaged with short-video social commerce and algorithm-driven content consumption. This demographic concentration is therefore considered appropriate for examining personalization and profiling behaviors within the TikTok Shop ecosystem.

4.2. Measurement model evaluation

The measurement model was evaluated by assessing the reliability and validity of the construct measures. Specifically, indicator reliability was examined through outer loadings, internal consistency reliability was assessed using Cronbach's alpha and composite reliability, convergent validity was evaluated through Average Variance Extracted (AVE), and discriminant validity was examined using both the HTMT ratio and the Fornell–Larcker criterion. Indicators with outer loadings above 0.70 are generally considered acceptable, while convergent validity is supported when AVE values exceed 0.50 (Hair et al., 2009). Discriminant validity was assessed using the HTMT threshold of 0.90 (Henseler et al., 2015) and further confirmed through the Fornell–Larcker criterion, where the square root of each construct's AVE should be greater than its correlations with other constructs (Fornell & Larcker, 1981) (*see Appendix 3 online*).

The research model includes 18 indicators across six constructs. After estimating the

measurement model, no indicators were removed because all outer loadings exceeded 0.70. Cronbach's alpha and composite reliability values were above the recommended thresholds, indicating satisfactory internal consistency. Convergent validity was established because all AVE values were above 0.50, showing that each construct explained more than half of the variance in its indicators. Discriminant validity was also supported, as all HTMT ratios in Appendix 4 (*see Appendix 4 online*) were below 0.90 and the Fornell–Larcker results in Appendix 5 (*see Appendix 5 online*) showed that the square root of AVE for each construct was higher than its inter-construct correlations.

4.3. Structural model evaluation

Before examining the structural relationships, collinearity diagnostics were assessed using VIF values. All reported VIF values ranged from 1.329 to 3.142, remaining below the threshold of 5.0, which indicates that collinearity is unlikely to distort the parameter estimates. These diagnostics suggest that the model is suitable for subsequent path analysis.

Table 1. The results of the structural model

Hypotheses	Coefficients (β)	p-values	f square	Support
H1: TP $\rightarrow$ PC	-0.038	0.754	0.001	Rejected
H2: TP $\rightarrow$ CT	0.317	0.000	0.149	Supported
H3: PA $\rightarrow$ PC	0.250	0.009	0.042	Rejected (opposite direction)
H4: PA $\rightarrow$ CT	0.365	0.000	0.211	Supported
H5a: OP $\rightarrow$ PC	0.309	0.002	0.062	Supported
H5b: OP $\rightarrow$ CT	0.258	0.000	0.101	Supported
H6: PC $\rightarrow$ WTBPO	0.120	0.007	0.028	Rejected (opposite direction)
H7: CT $\rightarrow$ WTBPO	0.566	0.000	0.409	Supported
H8: OP $\rightarrow$ WTBPO	0.201	0.002	0.046	Supported

The hypothesis testing results presented in Table 1 demonstrate a mixed but theoretically meaningful pattern across the proposed

research model. Out of the nine tested paths, six were supported, while three were not supported or were in the opposite direction.

Specifically, Technical Protection had a positive and significant effect on customer trust (H2: $\beta = 0.317$, $p < 0.001$, $f^2 = 0.149$), indicating a small-to-moderate practical effect. Privacy Awareness also positively affected customer trust (H4: $\beta = 0.365$, $p < 0.001$, $f^2 = 0.211$), supporting the proposed relationship and showing a moderate practical effect. Online Personalization positively influenced Privacy Concern (H5a: $\beta = 0.309$, $p = 0.002$, $f^2 = 0.062$) and customer trust (H5b: $\beta = 0.258$, $p < 0.001$, $f^2 = 0.101$), indicating that personalization simultaneously heightens privacy-related concern and strengthens trust in the platform.

Customer trust emerged as the most influential predictor of Willingness to be profiled online for Personalization (H7: $\beta = 0.566$, $p < 0.001$, $f^2 = 0.409$), indicating a large practical effect. Online Personalization also had a significant positive effect on Willingness to be profiled online (H8: $\beta = 0.201$, $p = 0.002$, $f^2 = 0.046$), although its effect size was relatively small. These results suggest that users' willingness to accept profiling on TikTok Shop is driven most strongly by customer trust, while personalization value also directly contributes to profiling acceptance.

However, several hypothesized relationships were not supported as expected. Technical Protection did not significantly reduce Privacy Concern (H1: $\beta = -0.038$, $p = 0.754$, $f^2 = 0.001$), indicating a negligible effect. Privacy Awareness had a positive, rather than negative, effect on Privacy Concern (H3: $\beta = 0.250$, $p = 0.009$, $f^2 = 0.042$), leading to the rejection of H3 in the opposite direction. Similarly, Privacy Concern positively affected willingness to be profiled online (H6: $\beta = 0.120$, $p = 0.007$, $f^2 = 0.028$), contrary to the expected negative relationship, although the practical effect was small.

Overall, the findings show that customer trust is the dominant substantive driver of

willingness to be profiled, whereas Privacy Concern has only a small positive effect. This supports the interpretation that privacy concern does not necessarily translate into resistance in short-video social commerce. Instead, users' acceptance of profiling on TikTok Shop appears to be shaped more strongly by platform trust and perceived personalization value, reflecting a context-specific personalization–privacy paradox.

Table 2. R^2 and predictive relevance (Q^2)

	R-square	R-square adjusted	Q^2
CT	0.673	0.669	0.540
PC	0.229	0.221	0.179
WTBPO	0.595	0.591	0.452

The explanatory and predictive power of the structural model was assessed using R^2 , Q^2 , and f^2 values. As shown in Table 2, the model explains 67.3% of the variance in customer trust, 59.5% of the variance in willingness to be profiled online for Personalization, and 22.9% of the variance in Privacy Concern. These results indicate substantial explanatory power for customer trust and moderate explanatory power for willingness to be profiled online, while Privacy Concern shows a more modest but acceptable level of explanation. In addition, all Q^2 values are above zero, with customer trust ($Q^2 = 0.540$), willingness to be profiled online ($Q^2 = 0.452$), and Privacy Concern ($Q^2 = 0.179$), confirming the predictive relevance of the model. Overall, these results suggest that the model has adequate explanatory and predictive capacity, with customer trust emerging as the most substantively important driver of users' willingness to accept profiling on TikTok Shop.

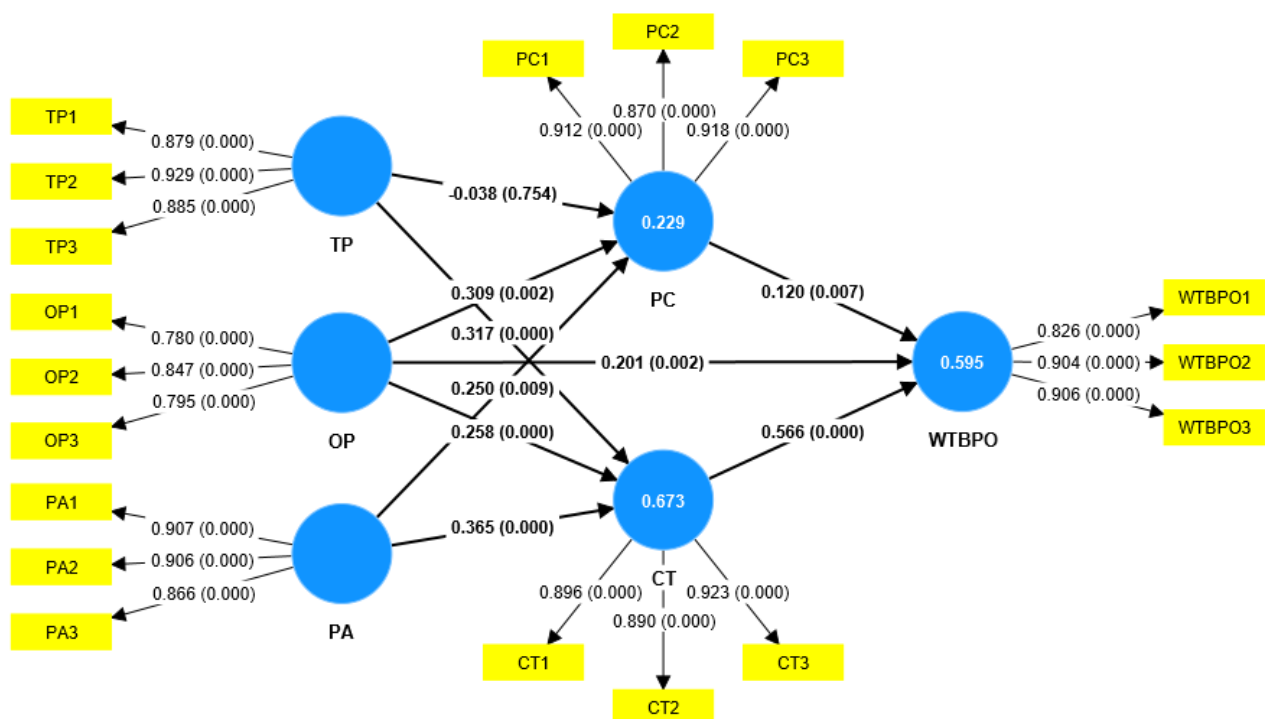
Table 3. The results of indirect effects

	Coefficients	T statistics	P values
OP → CT → WTBPO	0.146	4.522	0.000
TP → CT → WTBPO	0.179	5.502	0.000
PA → CT → WTBPO	0.206	6.044	0.000
OP → PC → WTBPO	0.037	2.145	0.032
TP → PC → WTBPO	-0.005	0.290	0.772
PA → PC → WTBPO	0.030	1.738	0.082

Table 3 reports the formal mediation test within the S-O-R framework. The results show that customer trust is the main Organism mechanism linking Stimulus factors to willingness to be profiled online. Specifically, Online Personalization ($\beta = 0.146$, $p < 0.001$), Technical Protection ($\beta = 0.179$, $p < 0.001$), and Privacy Awareness ($\beta = 0.206$, $p < 0.001$) all have significant indirect effects on willingness to be profiled online through customer trust. By contrast, Privacy Concern shows a weaker mediating role. Only the indirect effect of Online

Personalization through Privacy Concern is significant but small ($\beta = 0.037$, $p = 0.032$), while the indirect effects of Privacy Awareness ($\beta = 0.030$, $p = 0.082$) and Technical Protection ($\beta = -0.005$, $p = 0.772$) through Privacy Concern are not significant. These results suggest that users' willingness to accept profiling on TikTok Shop is explained more strongly by trust-based evaluations than by concern-based evaluations, thereby supporting the S-O-R logic of the proposed model.

4.4. Discussion

**Figure 2.** Structural model

The results provide a nuanced understanding of users' willingness to be profiled on TikTok Shop. Overall, customer trust emerges as the strongest determinant of willingness to be profiled online, while online personalization plays a dual role by increasing both privacy concern and customer trust. These findings suggest that users' acceptance of profiling in short-video social commerce is not shaped by privacy concern alone, but by the coexistence of personalization value, platform trust, and privacy-related awareness. This pattern is consistent with the personalization–privacy paradox, in which users may remain concerned about privacy while still accepting data-driven personalization when the perceived value of the platform experience is sufficiently strong.

Technical protection was found to have no significant effect on privacy concern but a significant positive effect on customer trust. This indicates that technical safeguards may not directly reduce users' concerns about data collection or platform profiling. In the TikTok Shop context, users may still worry about how their personal information is collected, analyzed, and shared, even when they perceive the platform as technically secure. However, Technical Protection appears to function as a trust-building signal. When users believe that the platform has adequate mechanisms to protect their data, they are more likely to view the platform as reliable and competent. This finding is consistent with prior studies suggesting that security and technical assurance mechanisms are important foundations of trust in online environments (Bélanger et al., 2002; Pavlou, 2003), although they may not be sufficient to eliminate privacy concern.

The results for Privacy Awareness are particularly important because they show two simultaneous effects. First, contrary to the proposed negative relationship, Privacy Awareness positively influences Privacy

Concern. This suggests that greater awareness does not necessarily reduce users' privacy concern in algorithm-driven social commerce. Instead, users who are more aware of data collection, tracking, and personalization practices may become more conscious of the extent to which their information is used by the platform. In this sense, awareness may intensify concern rather than reduce it, particularly when users recognize that TikTok Shop relies heavily on algorithmic profiling to deliver personalized content and product recommendations. This finding is consistent with the broader view that informed users may become more sensitive to privacy risks when they better understand how personal data are processed and used (Malhotra et al., 2004; Smith et al., 2011).

At the same time, Privacy Awareness positively affects customer trust, supporting the proposed hypothesis. This result suggests that awareness does not simply create suspicion; it may also help users evaluate the platform more rationally. When users understand why data are collected and how such data support personalized recommendations, they may perceive the platform as more transparent, functional, and competent. This is particularly relevant to TikTok Shop, where algorithmic recommendations are highly visible and closely connected to the shopping experience. Thus, privacy-aware users may simultaneously recognize privacy risks and trust the platform's ability to provide relevant and useful services. This dual effect helps explain why privacy awareness can increase both concern and trust in the same model.

Online Personalization also shows a dual effect. It significantly increases Privacy Concern, customer trust, and willingness to be profiled online. The positive effect on Privacy Concern indicates that personalized recommendations make users more aware that their data are being collected and analyzed. This supports the

logic of the personalization–privacy paradox, where the same personalization features that create value may also raise privacy-related concerns (Awad & Krishnan, 2006; Xu et al., 2011). However, Online Personalization also strengthens customer trust and directly increases willingness to be profiled online. This suggests that users may interpret personalization as evidence that the platform understands their preferences and provides relevant, convenient, and valuable recommendations. In the TikTok Shop context, where shopping is integrated with entertainment and continuous content discovery, personalization may be perceived not only as a privacy risk but also as a core benefit of platform use.

The positive relationship between Privacy Concern and willingness to be profiled online is another counter-intuitive finding. Although the effect size is small, the direction contradicts the traditional assumption that privacy concern should reduce willingness to disclose personal information. This result should not be interpreted as meaning that privacy concern is beneficial. Rather, it suggests that privacy concern does not necessarily translate into resistance in the TikTok Shop context. Users may remain concerned about privacy but still accept profiling when they perceive the benefits of personalized recommendations, convenience, entertainment, and platform trust as more important. This finding aligns with the privacy paradox literature, which shows that privacy concerns do not always lead to privacy-protective behavior (Norberg et al., 2007; Barth & de Jong, 2017).

This paradoxical pattern can also be understood through privacy resignation. In TikTok Shop, algorithmic profiling is not a peripheral feature but a central mechanism of product discovery and user engagement. Users may perceive data profiling as an unavoidable condition for receiving relevant

content, personalized offers, and a seamless shopping experience. As a result, they may tolerate privacy-related concerns not because they are unconcerned, but because opting out of profiling may reduce the value of using the platform. This interpretation is consistent with Draper and Turow's (2019) notion of digital resignation, where users continue to participate in data-driven environments despite concerns because they perceive limited meaningful alternatives.

Among all predictors, customer trust has the strongest effect on willingness to be profiled online. This finding confirms that trust is the key psychological mechanism that encourages users to accept profiling on TikTok Shop. When users believe that the platform is reliable, transparent, and capable of handling their information responsibly, they are more willing to allow their data to be used for personalized services. The mediation results further support this interpretation, showing that customer trust is the main Organism mechanism linking Stimulus factors to willingness to be profiled online. In contrast, Privacy Concern plays a weaker mediating role. This indicates that users' profiling acceptance is explained more strongly by trust-based evaluations than by concern-based evaluations.

Overall, the findings suggest that traditional privacy trade-off assumptions may not fully explain user behavior in short-video social commerce. In the TikTok Shop context, privacy concern, customer trust, and personalization value coexist rather than operate in a simple risk-versus-disclosure logic. Users may recognize privacy risks while still accepting profiling because algorithmic personalization is deeply embedded in the platform's entertainment, discovery, and shopping experience. Therefore, the study extends the personalization–privacy paradox by showing how profiling acceptance in algorithm-driven social commerce is shaped

less by privacy concern alone and more by the combined influence of trust, personalization value, and platform-specific user engagement.

5. Conclusion

5.1. Main Findings

The study shows that online personalization plays a dual role: it increases both privacy concern and customer trust, while also directly increasing willingness to be profiled. Technical protection strengthens customer trust but does not significantly reduce privacy concern. Privacy awareness unexpectedly increases privacy concern, while also positively affecting customer trust as hypothesized. Most notably, privacy concern is positively, rather than negatively, associated with willingness to be profiled, although this effect is weaker than that of customer trust. Overall, the findings suggest that users' willingness to accept profiling on TikTok Shop cannot be explained solely through traditional privacy-risk assumptions. Instead, acceptance of profiling appears to be shaped by the interplay among personalization value, customer trust, and privacy-related concerns within an algorithm-driven social commerce environment.

5.2. Implications

From a theoretical perspective, this study contributes to the personalization–privacy paradox literature by showing that privacy-related variables do not operate in a simple risk-reduction or resistance-based manner in short-video social commerce. By integrating Privacy Calculus Theory with the S-O-R framework, the study demonstrates that platform-related stimuli shape users' internal evaluations through both privacy concern and customer trust. In particular, the findings show that privacy awareness unexpectedly increases privacy concern while also strengthening customer trust, suggesting that users may become more

conscious of data risks and more confident in the platform at the same time. Moreover, customer trust emerges as the strongest predictor of willingness to be profiled, whereas privacy concern has only a small positive effect. These results suggest that traditional privacy calculus assumptions may not fully explain profiling acceptance in algorithm-driven social commerce, where personalization value, trust, and privacy-related unease can coexist.

From a managerial perspective, the findings suggest that TikTok Shop and similar platforms should prioritize customer trust as the key driver of users' acceptance of profiling. Technical protection alone may not reduce privacy concern, but it can strengthen trust when security practices are visible and understandable to users. Platforms should therefore communicate data protection mechanisms more clearly and transparently. In addition, personalization strategies should emphasize user value, such as relevant recommendations, convenience, and improved shopping experience, while avoiding excessive intrusiveness. Since personalization can simultaneously increase trust and privacy concern, platforms should combine personalized services with transparent explanations, consent options, and user control over personal data.

5.3. Limitations

Despite providing valuable insights, this study has several limitations. First, the study relied on a convenience sample of TikTok Shop users in Vietnam, with a strong concentration of respondents aged 18-24 and a high proportion of students. This sample structure limits the generalizability of the findings to the broader population of TikTok Shop users in Vietnam. Future research could employ probability sampling techniques and include broader populations to enhance the representativeness of the results.

Second, this study examined a limited set of variables related to personalization and privacy concerns. Future studies could extend the research model by incorporating additional factors such as perceived benefits, perceived risks, or platform reputation to provide a more comprehensive understanding of the personalization–privacy paradox. Furthermore, comparative studies across different social commerce platforms or countries could offer deeper insights into how cultural and technological contexts influence consumer privacy perceptions and data-sharing behavior.

In addition, the cross-sectional nature of the study limits the ability to observe how privacy perceptions and profiling acceptance may evolve. Future longitudinal studies could provide deeper insights into the dynamic relationship between personalization, trust, and privacy-related behaviors in social commerce environments.

Furthermore, concepts such as privacy resignation and perceived reciprocity were used as interpretive explanations in the discussion but were not directly measured in the research model. Future studies could incorporate these constructs to provide a more comprehensive

explanation of profiling acceptance behaviors in algorithm-driven commerce platforms.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

AI Usage Statement

During manuscript preparation, the authors used ChatGPT (OpenAI) for language editing, structural support, and reference-format checking. The authors reviewed and edited the output and take full responsibility for the final content.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

AI Usage Statement

During manuscript preparation, the authors used ChatGPT (OpenAI) for language editing, structural support, and reference-format checking. The authors reviewed and edited the output and take full responsibility for the final content.

References

- 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. <https://doi.org/10.2307/25148715>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern, and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138–150. <https://doi.org/10.1016/j.dss.2010.01.010>
- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- 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>
- Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3–4), 245–270. [https://doi.org/10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5)
- Bleier, A., & Eisenbeiss, M. (2015). Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science*, 34(5), 669–688. <https://doi.org/10.1287/mksc.2015.0930>

- Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15(5-6), 358–368. <https://doi.org/10.1108/09576050210447046>
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2–3), 181–202. <https://doi.org/10.1007/s10799-005-5879-y>
- 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>
- Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, 21(8), 1824–1839. <https://doi.org/10.1177/1461444819833331>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>
- 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>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate data analysis* (7th ed.). Pearson.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Hoang, V. T., & Dang, H. P. (2024). Exploring how the characteristics of live streaming affect impulse buying behaviour in live streaming commerce: The mediating effect of trust and flow experience. *International Journal of Business Science and Applied Management*, 19(1), 77–93. <https://doi.org/10.69864/ijbsam.19-1.184>
- Kezer, M., Dienlin, T., & Baruh, L. (2022). Getting the privacy calculus right: Analyzing the relations between privacy concerns, expected benefits, and self-disclosure using response surface analysis. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16(4). <https://doi.org/10.5817/CP2022-4-1>
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. *Information Systems Research*, 20(2), 237–257. <https://doi.org/10.1287/isre.1080.0188>
- Kim, S. S. (2020). Purchase intention in the online open market: Do concerns for e-commerce really matter? *Sustainability*, 12(3). <https://doi.org/10.3390/su12030773>
- Le, M. T. H., Pham, H. N. M., Nguyen, L. T. T., Le, T. T. X., & Nguyen, S. T. M. (2025). Augmenting TikTok Shop adoption: The mediating role of key opinion consumers (KOCs) in live streaming, video content, and artificial intelligence (AI) recommendations. *Ho Chi Minh City Open University Journal of Science – Economics and Business Administration*, 15(2), 85–104. <https://doi.org/10.46223/HCMCOUJS.econ.en.15.2.2939.2025>
- Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, 21(6), 621–642. <https://doi.org/10.1057/ejis.2012.13>
- Lwin, M. O., Wirtz, J., & Stanaland, A. J. S. (2016). The privacy dyad: Antecedents of promotion- and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern. *Internet Research*, 26(4), 919–941. <https://doi.org/10.1108/IntR-05-2014-0134>
- 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>
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. <https://doi.org/10.1007/s11747-016-0495-4>
- Melgarejo-Espinoza, R., Gonzales-Cruz, M., Chavez-Perez, J., & Iparraguirre-Villanueva, O. (2025). Impact of the TikTok algorithm on the effectiveness of marketing strategies: A study of consumer behavior and content preferences. *International Journal of Advanced Computer Science and Applications*, 16(2), 147–156. <https://doi.org/10.14569/IJACSA.2025.0160215>
- 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>
- Pappas, I. O., Kourouthanassis, P. E., Giannakos, M. N., & Chrissikopoulos, V. (2014). Shiny happy people buying: The role of emotions on personalized e-shopping. *Electronic Markets*, 24(3), 193–206. <https://doi.org/10.1007/s12525-014-0153-y>

- 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>
- Sah, J., & Jun, S. (2024). The role of consumers' privacy awareness in the privacy calculus for IoT services. *International Journal of Human-Computer Interaction*, 40(12), 3173–3184. <https://doi.org/10.1080/10447318.2023.2184102>
- Saha, R. K., & Ali, M. B. (2024). Does enduring brand loyalty in mobile financial service platforms require strong commitment? A stimulus–organism–response (S-O-R) perspective. *Journal of Financial Services Marketing*, 29(4), 1623–1634. <https://doi.org/10.1057/s41264-024-00289-1>
- Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. *International Journal of Information Management*, 34(1), 48–57. <https://doi.org/10.1016/j.ijinfomgt.2013.10.001>
- 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>
- Tam, K. Y., & Ho, S. Y. (2006). Understanding the impact of web personalization on user information processing and decision outcomes. *MIS Quarterly*, 30(4), 865–890. <https://doi.org/10.2307/25148757>
- Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision-making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52. <https://doi.org/10.1016/j.dss.2010.11.017>