Journal of
Theoretical and Applied Electronic Commerce Research

MDPI

Article

Perceived Privacy Invasion and Consumer Adoption Willingness of AI-Powered Personalized Recommendations: The Mediating Role of Psychological Resistance and Moderating Role of Perceived Algorithm Transparency

Xiaolan Zhu [1], Siwarit Pongsakornrungsilp [2,*], Pimlapas Pongsakornrungsilp [3] and Yuksel Ekinci [2,4]

[1] College of Low-Altitude Economy and Business, Guangzhou Huashang Vocational College, Guangzhou 511300, China; xiaolanzhu@gzhsvc.edu.cn
[2] Center of Excellence for Tourism Business Management and Creative Economy, Department of Digital Marketing, School of Management, Walailak University, Nakhon Si Thammarat 80160, Thailand; yuksel.ekinci@port.ac.uk
[3] Center of Excellence for Tourism Business Management and Creative Economy, Department of Tourism and Prochef, School of Management, Walailak University, Nakhon Si Thammarat 80160, Thailand; kpimlapa@wu.ac.th
[4] Faculty of Business and Law, University of Portsmouth, Portsmouth PO1 2EG, UK
* Correspondence: psiwarit@wu.ac.th; Tel.: +66-75-672201

Abstract

Artificial intelligence (AI)-powered personalized recommendation systems can enhance relevance and convenience, but their reliance on extensive personal data processing may also heighten users' perceptions of privacy intrusion. This study examines the relationship between perceived privacy invasion and consumer adoption willingness, with psychological resistance as a statistical mediator and perceived algorithm transparency (PAT) as a moderating condition. Drawing on the privacy-cost perspective of privacy calculus theory and psychological reactance theory, this study focuses on the privacy-related inhibition pathway of AI recommendation adoption. Survey data were collected from 518 Chinese adult Internet users with recent experience of AI-powered personalized recommendation services and analyzed using partial least squares structural equation modeling (PLS-SEM). The results show that perceived privacy invasion was negatively associated with consumer adoption willingness ($\beta = -0.357$) and positively associated with psychological resistance ($\beta = 0.279$), whereas psychological resistance was negatively associated with adoption willingness ($\beta = -0.286$). Psychological resistance statistically partially mediated the association between perceived privacy invasion and adoption willingness (indirect effect = -0.080). The interaction between perceived privacy invasion and PAT was negative and statistically significant ($\beta = -0.162$), indicating that the positive privacy invasion–resistance association was less pronounced at higher levels of PAT. Supplementary conditional process analysis further showed that the negative indirect association through psychological resistance weakened as PAT increased, with a significant index of moderated mediation (index = 0.0464, 95% bootstrap CI [0.0191, 0.0816]). Additional analyses using common-method-bias diagnostics, PLSpredict and CVPAT, and a targeted Gaussian copula robustness check for PAT provided complementary evidence regarding measurement robustness, predictive relevance, and the robustness of PAT-related estimates. Age-based multigroup analysis revealed no statistically significant age-based heterogeneity in the structural path coefficients across the 18–29, 30–49, and 50+ age groups. This study contributes to the literature by identifying psychological resistance as a motivational pathway associated with privacy-related adoption responses and by conceptualizing PAT as a user-level perceptual boundary condition in AI-powered personalized recommendation contexts.

Academic Editors: Hua Pang and Lian Zhu

Received: 26 July 2026
Revised: 1 September 2026
Accepted: 1 September 2026
Published: 6 September 2026

Keywords: AI-powered personalized recommendation; perceived privacy invasion; psychological resistance; consumer adoption willingness; perceived algorithm transparency; privacy calculus; psychological reactance

1. Introduction

Artificial intelligence (AI) has become deeply embedded in digital commerce and platform ecosystems, especially in e-commerce, social media, and online content distribution [1]. One of its most influential applications is AI-powered personalized recommendations, which use consumer data to infer preferences, tailor content, and support online decision-making [2]. Previous studies have suggested that personalization can improve information matching, reduce search effort, and enhance the effectiveness of recommendation services [3,4]. Recent studies, including work published in the Journal of Theoretical and Applied Electronic Commerce Research, further show that AI-powered personalized recommendations are closely associated with consumer clicking intentions, spontaneous buying responses, and broader behavioral evaluations across e-commerce and short-form video environments [4–6]. Thus, AI recommendations have become a crucial way for consumers to be exposed to products/services and information in algorithm-mediated environments [1,2].

A recent empirical study also indicated that perceived accuracy is a significant value-enhancing mechanism when it comes to personalized AI recommendations. For instance, Zhu et al. [7] discovered that perceived accuracy positively affects the degree of consumer willingness to adopt the product directly, in addition to indirectly by influencing perceived benefit; product involvement moderates this effect. These findings highlight the benefit-oriented pathway through which AI recommendation systems promote adoption.

These benefits notwithstanding, AI-driven personalized recommendation is not necessarily seen as an unquestionably good technology [8,9]. It relies on ongoing data collection, integration, and processing of personal information, which can lead to feelings of discomfort, vulnerability, and being intruded upon [8,10,11]. Personalized outputs can be seen as an intrusion if the users think the recommendation system knows too much about them. This tension is indicative of the personalization–privacy paradox, which states that the same personalization practices that make things more relevant and useful can also make people more aware and concerned about privacy issues, and more negative or less positive about the experience [8,9,12–14]. Recent research has further suggested that acceptance of the recommendations is dependent upon how beneficial the personalization is versus their concerns with privacy violation and that privacy-preserving or explainable interventions can have a meaningful impact on reducing perceived privacy violation in digital consumption situations [15,16].

Against this background, consumer adoption willingness becomes a critical outcome in AI-powered recommendation contexts [3,17]. Adoption willingness reflects whether users are willing to accept, rely on, and continue using AI-generated recommendations in actual consumption settings [3,17,18]. Existing studies suggest that responses to algorithmic systems are shaped not only by performance-related evaluations, but also by trust, transparency, explainability, and privacy perceptions [3,11,17,19]. In this sense, perceived privacy invasion may represent a major barrier to adoption [8,11,20]. Once users perceive that a recommendation system has crossed the boundary between personalization and intrusion, their willingness to accept and use that system may decline substantially [8,9,21].

Although this relationship is increasingly relevant, the literature has not yet fully explained how perceived privacy invasion is associated with lower consumer adoption willingness in AI-powered personalized recommendation contexts. Prior research on personalization and privacy has mainly focused on privacy concern, trust, perceived risk, or communication effectiveness, often showing that excessive or covert information collection is associated with less favorable user responses [8,9,21]. Related work on information privacy has similarly demonstrated that perceptions of privacy are associated with behavioral intentions and willingness to engage in online transactions [11,20]. However, compared with the expanding literature on the value-enhancing role of AI recommendations, the privacy-related inhibition pathway remains less developed, particularly with respect to the psychological process that may statistically link perceived privacy invasion with adoption willingness [2–4].

One important missing link is psychological resistance. Grounded in psychological reactance theory, psychological resistance refers to a negative motivational state that may arise when individuals perceive that their freedom, autonomy, or control is being restricted or manipulated [22,23]. In AI-powered recommendation settings, users may not only be concerned about privacy in an abstract sense; they may also experience psychological resistance when personalized recommendations create the impression that the system is overly intrusive, difficult to control, or steering their choices without sufficient authorization [9,12,22,23]. Under such conditions, stronger perceived privacy invasion may be associated with greater discomfort, defensiveness, and resistance, which may in turn be associated with lower willingness to adopt AI recommendations [9,11,23]. However, prior research has rarely examined psychological resistance as a statistical mediating pathway linking perceived privacy invasion with consumer adoption willingness in AI-powered personalized recommendation contexts.

A second unresolved issue concerns perceived algorithm transparency (PAT). Prior research suggests that transparency and explainability are associated with users' trust, perceived legitimacy, and acceptance of AI systems [3,17,24]. In the present study, PAT refers specifically to the extent to which users perceive that they understand how and why recommendations are generated, what information is used, and how the system arrives at personalized outputs [17,25]. Greater perceived transparency may provide interpretive cues that reduce uncertainty surrounding recommendation logic and data use. Accordingly, PAT may serve as a user-level perceptual boundary condition in the association between perceived privacy invasion and psychological resistance [3,17]. Although transparency has received growing attention, its moderating role in the privacy invasion–resistance relationship remains comparatively underexplored in consumer-facing AI recommendation contexts [17,24,25].

A further empirical question concerns potential age-based heterogeneity in these relationships. Much of the prior literature on AI recommendation adoption has focused on younger or digitally experienced users, even though AI-powered recommendation services are increasingly used by a broader population [1,17,26]. It therefore remains useful to examine whether statistically detectable differences in the proposed privacy–resistance–adoption relationships emerge across age groups. Rather than assuming age-based heterogeneity a priori, the present study treats age-based multigroup analysis as an exploratory assessment of potential structural heterogeneity rather than as a test of structural equivalence or generalizability.

Against this background, the present study examines the relationship between perceived privacy invasion and consumer adoption willingness in AI-powered personalized recommendation contexts. More specifically, this study develops and tests a first-stage moderated mediation framework in which perceived privacy invasion is expected to be negatively associated with consumer adoption willingness, psychological resistance statistically mediates this association, and perceived algorithm transparency moderates the positive association between perceived privacy invasion and psychological resistance. In addition, the study evaluates whether statistically detectable heterogeneity in these structural relationships exists across three age groups (18–29, 30–49, and 50+). Drawing on the privacy-cost perspective of privacy calculus theory and psychological reactance theory, this study therefore seeks to clarify both the motivational pathway associated with privacy-related responses and the perceptual condition under which the privacy invasion–resistance association may be attenuated.

This study contributes to the literature in four ways. First, it advances research on AI-powered personalized recommendations by complementing the dominant value-enhancing perspective with a privacy-related inhibition perspective. Rather than focusing only on why consumers accept AI recommendations, this study examines why stronger perceptions of privacy invasion are associated with lower adoption willingness in data-intensive personalization contexts [2,4,17]. Second, the study contributes to privacy research by focusing on perceived privacy invasion as an immediate perception of boundary crossing and by examining psychological resistance as a motivational response associated with that perception. Rather than treating privacy-related responses only as broad evaluations of potential privacy risk, the proposed framework links perceived boundary violation with an autonomy-related resistance response [22,23]. General privacy concern, however, is not measured as a separate construct in this study; therefore, the distinction between perceived privacy invasion and general privacy concern is conceptual rather than an empirically tested discriminant distinction. Third, the study extends psychological reactance theory to AI-powered personalized recommendation by testing psychological resistance as a statistical mediating pathway between perceived privacy invasion and consumer adoption willingness. This provides a more specific account of how privacy-related perceptions may be associated with adoption willingness through an intervening motivational response. Fourth, the study contributes to research on algorithm transparency by conceptualizing perceived algorithm transparency as a user-level perceptual boundary condition rather than an objective platform governance property. By testing whether the privacy invasion–resistance association varies with users' perceived understanding of recommendation logic, data use, and explanations, this study extends research on transparency beyond its commonly examined direct associations with trust and acceptance. More specifically, the study examines whether PAT conditions not only the first-stage privacy invasion–resistance association but also the corresponding indirect association between perceived privacy invasion and adoption willingness through psychological resistance.

The remainder of this paper is structured as follows. Section 2 reviews the relevant literature and develops the hypotheses. Section 3 presents the research methodology, including sampling, measurement, and data analysis procedures. Section 4 reports the empirical findings. Section 5 discusses the theoretical and practical implications of the results. Section 6 concludes the study and discusses its theoretical contributions, managerial implications, limitations, and directions for future research.

2. Literature Review and Hypothesis Development

2.1. Theoretical Background

This study is theoretically grounded in privacy calculus theory and psychological reactance theory, with the personalization–privacy paradox used as the contextual background for understanding AI-powered personalized recommendation. Privacy calculus theory provides a basis for understanding perceived privacy invasion as a privacy-related cost that may be negatively associated with consumer adoption willingness. Psychological reactance theory can be used to understand why users may react psychologically to the invasion of their privacy and thus limit their willingness to adopt because they feel their autonomy, freedom, and perceived control have been threatened. The logical underpinning of the personalization–privacy paradox is the notion that AI-driven personalization can generate value and exacerbate privacy concerns at the same time. It should be noted that this study does not try to test the entire benefit–cost structure of privacy calculus theory. Rather, it looks at the privacy-cost side of the privacy calculus theory by examining the direct and indirect associations of perceived privacy invasion with consumer adoption willingness toward AI-powered personalized recommendations.

According to privacy calculus theory, consumers assess digital services based on the benefits that they perceive and the costs or risks that they perceive related to privacy [11]. This perspective has theoretical foundations in social exchange theory, which argues that social behavior is an exchange process that is influenced by rewards and costs [27]. The logic of these early privacy studies was extended by privacy research questioning disclosure, which posits that disclosure is based on behavioral calculus by comparing the expected benefits with the possible privacy losses [28,29]. Subsequent research on information systems has explored this view in online environments and found that the perceived benefits, privacy concerns, and online trust cues are all factors to consider in privacy-related decision-making [11,19,20].

This perspective is particularly relevant in AI-powered personalized recommendation environments because recommendation effectiveness depends on the extensive collection and use of personal data [3,11,19]. Although such data use may improve relevance and convenience, it may also raise perceptions of privacy intrusion, vulnerability, and reduced control [9,10]. Recent studies have further shown that recommendation acceptance increasingly depends on how users balance personalization benefits against privacy-related risks in data-intensive digital environments [14,15]. Therefore, privacy-related evaluations are likely to play an important role in shaping consumers' willingness to accept AI-generated recommendations [11,17,20].

At the same time, privacy-related perceptions do not operate only through rational cost–benefit evaluation. Psychological reactance theory argues that when individuals perceive threats to their freedom, autonomy, or control, they may develop a negative motivational state characterized by resistance, defensiveness, and opposition [22,23]. This perspective is useful for explaining why users may respond negatively to AI-powered personalized recommendation systems when they feel that such systems are excessively intrusive or manipulative [9,22]. Recent studies on digital personalization and AI-mediated interaction also suggest that privacy threats may be associated with discomfort, skepticism, and withdrawal responses. In this sense, privacy invasion may also be associated with psychological resistance in an affective and motivational sense [12,14,30].

Research on transparent and explainable AI further suggests that transparency can shape user perceptions of trust, legitimacy, and acceptance [3,17,24]. In recommendation settings, transparency may reduce uncertainty about how recommendations are generated and thus weaken users' suspicion that they are being covertly monitored or manipulated [17,25]. More recent studies also indicate that transparency signaling can improve trusting beliefs and advice utilization in algorithmic systems, especially when users are uncertain about data usage and recommendation logic [25,31,32]. Accordingly, perceived algorithm transparency may function as an important boundary condition in the relationship between perceived privacy invasion and psychological resistance.

Based on these theoretical perspectives, this study proposes a privacy-related inhibition framework in which perceived privacy invasion is expected to be negatively associated with consumer adoption willingness both directly and indirectly through psychological resistance. Perceived algorithm transparency is further proposed as a boundary condition that moderates the positive association between perceived privacy invasion and psychological resistance, such that this association is weaker at higher levels of perceived algorithm transparency.

2.2. Perceived Privacy Invasion and Consumer Adoption Willingness

Perceived privacy invasion refers to users' subjective perception that the collection, inference, or use of their personal information crosses acceptable privacy boundaries or feels excessively intrusive [8,11,20]. In AI-powered personalized recommendation environments, users often recognize that recommendation systems rely on behavioral data, browsing histories, interaction patterns, and inferred preferences to generate tailored outputs [2,3]. However, when such personalization becomes too precise or too intrusive, users may feel that the system has crossed the boundary between relevance and intrusion [8,9]. Under these conditions, the recommendation process may be viewed less as a helpful service and more as an unwelcome form of surveillance [8,12].

Prior research has consistently shown that privacy-related concerns can reduce favorable responses to personalized digital communication [8,9,21]. Studies on online personalization and targeted advertising have shown that excessive information collection may undermine trust and reduce user acceptance [8,9]. Research on information privacy has similarly shown that privacy perceptions influence behavioral intention and willingness to engage in online transactions or information disclosure [11,20,33]. More recent studies in AI-enabled recommendation contexts have further shown that consumers' recommendation acceptance depends on how they resolve the personalization–privacy paradox and whether privacy-preserving or control-enhancing mechanisms are present [15,16]. Recent research further suggests that AI-enabled personalization may simultaneously create value while heightening perceptions of surveillance, privacy violation, and privacy-related risk, reinforcing the need to examine the downside of personalized commerce [34,35]. In the context of AI-powered recommendation, this logic suggests that when users perceive recommendation systems as privacy-invasive, they are less likely to accept, rely on, or continue using them [3,17]. Accordingly, perceived privacy invasion is expected to be negatively associated with consumer adoption willingness.

H1. *Perceived privacy invasion in AI-powered personalized recommendations is negatively associated with consumer adoption willingness.*

2.3. Perceived Privacy Invasion and Psychological Resistance

Although perceived privacy invasion may be directly associated with lower willingness to adopt AI recommendations, its association with adoption willingness may also involve a more immediate psychological response. According to psychological reactance theory, individuals tend to resist situations in which they perceive that their freedom, autonomy, or behavioral control is being constrained [22,23]. In digital recommendation environments, privacy invasion may create such a perception because users may feel that the system is monitoring them too closely, shaping their choices in opaque ways, or narrowing their decision space without explicit authorization [12].

Prior personalization research has shown that consumers may react negatively when data use practices appear overly intrusive or manipulative [8,9]. These findings imply that perceived privacy invasion may be associated not only with cognitive concern, but also with a stronger motivational response in the form of psychological resistance. In AI-powered recommendation contexts, users who feel that recommendations are generated through excessive or intrusive data practices may become defensive, suspicious, and resistant toward the system [12,14]. This interpretation is also consistent with recent consumer-behavior research emphasizing consumer autonomy threat as an important concern in AI marketing and AI-based promotions. When AI-driven promotional or recommendation practices are perceived as constraining consumers' freedom of choice or exerting excessive influence over their decisions, autonomy-related resistance may become particularly salient [36]. Recent studies have also emphasized that privacy intrusiveness in interactive digital environments can heighten psychological resistance and reduce engagement, particularly when personalization is perceived as manipulative or uncontrollable [30,37]. Therefore, perceived privacy invasion is expected to be positively associated with psychological resistance.

H2. *Perceived privacy invasion in AI-powered personalized recommendations is positively associated with psychological resistance.*

2.4. Psychological Resistance and Consumer Adoption Willingness

Psychological resistance reflects a negative motivational state in which individuals oppose or avoid a system because they perceive it as controlling, intrusive, or manipulative [22,23]. In AI-powered recommendation settings, such resistance is likely to be associated with lower willingness to accept and use recommendation outputs [3]. Even if a recommendation system is functionally effective, users may hesitate to adopt it when they feel discomfort, suspicion, or defensiveness toward the recommendation process itself [12].

This argument is consistent with the broader literature on user responses to algorithmic systems. Studies on explainable AI and algorithmic interaction suggest that trust, transparency, and perceived legitimacy are important preconditions of acceptance [3,17,24]. When these conditions are weakened and users instead experience resistance, adoption willingness is likely to decline [3,17]. Recent studies in AI and digital service environments also show that psychological resistance can suppress sustained use, engagement, and supportive behavioral intention when users feel that system decisions undermine autonomy or comfort [38,39]. In this sense, psychological resistance represents a critical negative mechanism through which users withdraw from algorithmically mediated services. Accordingly, psychological resistance is expected to be negatively associated with consumer adoption willingness.

H3. *Psychological resistance is negatively associated with consumer adoption willingness.*

2.5. The Mediating Role of Psychological Resistance

The above arguments suggest that perceived privacy invasion may be negatively associated with adoption willingness both directly and indirectly through psychological resistance. When users perceive AI-powered personalized recommendation as being overly intrusive, they may feel that the system threatens their autonomy or exceeds acceptable boundaries of personalization [8,9,12]. This perception may be associated with heightened psychological resistance, which in turn may be associated with lower willingness to adopt the recommendation system.

Compared with privacy-focused models that primarily emphasize broader risk or concern evaluations, the present framework focuses on perceived privacy invasion as an immediate boundary-crossing perception and psychological resistance as an autonomy-related motivational response associated with that perception. This formulation does not empirically compare perceived privacy invasion with general privacy concern; rather, it specifies the particular privacy-related perception examined in the present model and the motivational pathway through which it is statistically associated with adoption willingness [11,23]. Recent research on AI personalization, recommendation systems, and intelligent assistants has similarly suggested that privacy concern often influences user behavior through intermediate emotional or motivational responses, rather than through direct evaluation alone [40–42]. Thus, the mediating role of psychological resistance helps clarify the internal process through which privacy invasion becomes behaviorally consequential in AI-powered recommendation environments. Therefore, psychological resistance is expected to mediate the negative association between perceived privacy invasion and consumer adoption willingness.

H4. *Psychological resistance mediates the negative association between perceived privacy invasion and consumer adoption willingness.*

2.6. The Moderating Role of Perceived Algorithm Transparency

Perceived algorithm transparency (PAT) refers to the extent to which users perceive that they can understand how and why an AI system generates personalized recommendations, what information is used in the recommendation process, and whether understandable explanations are available when needed [17,25]. In the present study, PAT is therefore conceptualized as a user-level perceptual construct, rather than as an objective property of an algorithm or a direct measure of platform governance. This distinction is important because users may differ in their perceptions of transparency even when they interact with the same technical system.

Prior research suggests that greater perceived transparency and explainability are associated with stronger trust, perceived legitimacy, and acceptance of AI systems because they reduce uncertainty regarding how algorithmic decisions are produced [3,17,24,25]. Recent *JTAER* research on e-commerce recommendation systems likewise highlights AI transparency as an important informational and perceptual factor associated with user evaluation and behavioral responses [43]. In personalized recommendation environments, users may be particularly sensitive to uncertainty surrounding data use, inferred preferences, and recommendation logic. When users perceive that they understand why specific content is recommended and how relevant data are used, the recommendation process may appear less opaque and less difficult to interpret.

This perceptual clarity may be particularly relevant when users already experience privacy-related concerns. Perceived privacy invasion reflects the sense that personal data practices have crossed acceptable privacy boundaries, whereas perceived algorithm transparency reflects the extent to which users believe that the recommendation process is understandable and explainable. Although transparency does not eliminate the perception of privacy invasion itself, greater PAT may provide users with interpretive cues that reduce ambiguity surrounding the recommendation process. As a result, a given level of perceived privacy invasion may be associated with a less pronounced psychological resistance response when perceived algorithm transparency is relatively high.

By contrast, when perceived algorithm transparency is low, users have fewer interpretive cues for understanding how recommendations are generated or why particular personal information appears to have been used. Under such conditions, perceived privacy invasion may be more strongly associated with suspicion, defensiveness, and psychological resistance. Thus, PAT is conceptualized as a perceptual boundary condition that may attenuate the positive association between perceived privacy invasion and psychological resistance.

Accordingly, this study proposes that perceived algorithm transparency negatively moderates the association between perceived privacy invasion and psychological resistance, such that the positive association is weaker at higher levels of perceived algorithm transparency.

H5. *Perceived algorithm transparency negatively moderates the association between perceived privacy invasion and psychological resistance, such that the positive association between perceived privacy invasion and psychological resistance is weaker at higher levels of perceived algorithm transparency.*

Taken together, the proposed first-stage moderation implies a conditional indirect association. If perceived algorithm transparency weakens the positive association between perceived privacy invasion and psychological resistance, then the negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance should also become weaker as perceived algorithm transparency increases. Accordingly, this study proposes the following moderated mediation hypothesis.

H6. *The negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance is weaker at higher levels of perceived algorithm transparency.*

2.7. Research Model

Based on the above theoretical arguments, this study proposes a first-stage moderated mediation model as shown in Figure 1.

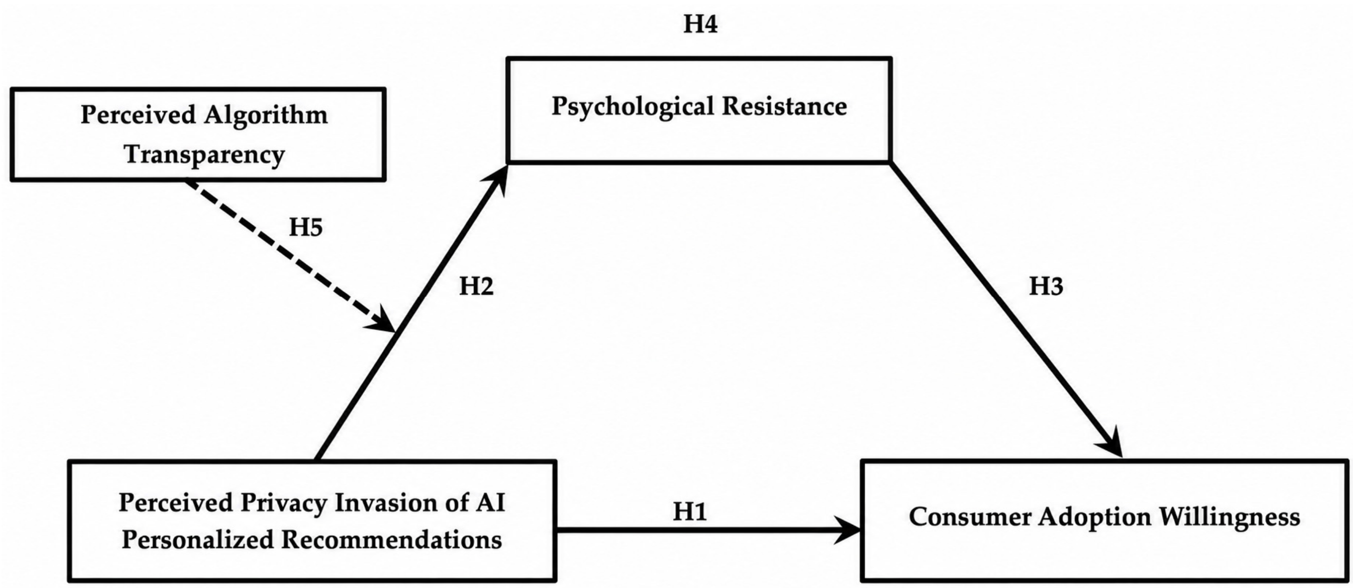

Figure 1. Research model. Note: H4 represents the statistical mediating role of psychological resistance in the association between perceived privacy invasion and consumer adoption willingness. H5 represents the first-stage moderating role of perceived algorithm transparency in the association between perceived privacy invasion and psychological resistance. H6 represents the moderated mediation hypothesis, whereby the negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance is expected to become weaker at higher levels of perceived algorithm transparency. H6 is tested statistically through conditional indirect effects and the index of moderated mediation and is therefore not represented by a separate structural path in the figure.

The overall model examines how perceived privacy invasion is associated with consumer adoption willingness, the statistical mediating role of psychological resistance in this relationship, and the conditions under which the privacy invasion–resistance association may be attenuated. Perceived privacy invasion is expected to be negatively associated with consumer adoption willingness (H1) and positively associated with psychological resistance (H2), while psychological resistance is expected to be negatively associated with adoption willingness (H3) and to mediate the PV–AW association (H4). It is also proposed that perceived algorithm transparency moderates the PV–PR association such that this positive association is weaker at higher levels of PAT (H5). Building on this first-stage moderation, the model further proposes that the negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance becomes weaker as PAT increases (H6).

Age was additionally examined as a potential source of heterogeneity in the structural relationships. Prior technology-adoption research suggests that generational groups may differ in the motivational factors, consumption values, and behavioral intentions associated with digital-service adoption [44]. However, chronological age alone may not fully capture these underlying motivational or value-based differences. Accordingly, the age-based multi-group analysis in the present study was treated as an exploratory assessment of whether statistically detectable structural differences emerged across the three age categories, rather than as a test of deterministic generational effects.

3. Methodology

This study employs a quantitative research design according to the positivist paradigm, which emphasizes the objective measurement and statistical validation of relationships between variables [45]. This approach is appropriate for examining the relationships between perceived privacy invasion, psychological resistance, perceived algorithm transparency, and consumer adoption willingness, as it enables systematic hypothesis testing and statistical assessment of the proposed relationships.

3.1. Sampling Methods

The target population of this study comprised adult Chinese consumers with experience using AI-powered personalized recommendation systems on digital platforms, including e-commerce platforms (e.g., Taobao, JD.com, and Pinduoduo), short-video platforms (e.g., Douyin and Kuaishou), social/content platforms (e.g., Xiaohongshu and Weibo), and travel-service applications (e.g., Ctrip). Respondents were required to have recent experience with AI-powered personalized recommendation services so that they could meaningfully evaluate the focal constructs examined in this study [46]. Given the geographically dispersed nature of the target population, convenience sampling was employed together with screening questions. The screening process collected information on respondents' prior experience with AI-powered personalized recommendations as well as demographic characteristics, including age, gender, region, and educational level. To reduce the tendency of technology-adoption research to overrepresent younger users, attention was given to achieving broader age coverage during recruitment [26]. According to recent statistics released by the China Internet Network Information Center (CNNIC), Internet use among middle-aged and older adults has become increasingly substantial [47]. Accordingly, the final sample included respondents across a broad age range, providing a basis for the subsequent age-based robustness and multigroup analyses.

The minimum sample size was determined using the inverse square root method, a standard approach for PLS-SEM studies [48,49]. The formula is as follows:

$$\mathrm{n_{min}} > \left(\frac{\mathrm{Z}}{\mathrm{P_{min}}}\right)^2 \tag{1}$$

In this approach, 2.486 represents the constant corresponding to a 5% significance level and 80% statistical power, while $\mathrm{P_{min}}$ denotes the smallest path coefficient that the model is intended to detect. In the present study, $\mathrm{P_{min}}$ was conservatively set at 0.11 to allow the detection of relatively small but meaningful structural relationships. This selection was made based on the synthesis of empirical studies on the factors affecting users' adoption intention towards personalized algorithm recommendation services in the meta-analysis conducted by Shi et al. [50]. Since the current study also looks at consumer adoption willingness in the context of AI-based personalized recommendations, $\mathrm{P_{min}}$ = 0.11 was deemed to be a suitable value for capturing relatively smaller, yet meaningful, structural effects. The formula was then evaluated using this value and, based on the inverse square root method, resulted in a minimum sample size of approximately 511.

$$n_{\min} > \left(\frac{2.486}{0.11}\right)^2 \approx 511 \quad (2)$$

Based on the inverse square root method, the required minimum sample size was approximately 511. Recruitment therefore aimed to obtain a final analytical sample exceeding this threshold after eligibility and data-quality screening [51,52].

3.2. The Research Instrument

The measurement items in this study were adapted from well-established scales in the prior literature and revised to fit the context of AI-powered personalized recommendation services. All items were measured using a five-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree. The measurement items and their literature sources are provided in Appendix A (Table A1), which also reports the standardized indicator loadings, Cronbach's alpha, rho_A, composite reliability (rho_C), and average variance extracted (AVE). The English scale items were translated into Chinese where necessary and checked through a back-translation procedure by bilingual researchers to ensure semantic equivalence. Minor wording adjustments were made to improve contextual fit without changing the conceptual meaning of the original items.

In interpreting the adapted measures, the four constructs were conceptually distinguished according to their intended roles in the proposed model. Perceived privacy invasion was operationalized as users' subjective perception that personal-data practices cross acceptable privacy boundaries. Psychological resistance was intended to capture autonomy-related aversive and oppositional responses toward recommendation practices perceived as intrusive, controlling, or manipulative. Perceived algorithm transparency reflected users' perceived understanding of recommendation logic, data use, and available explanations, whereas consumer adoption willingness captured behavioral willingness to engage with, accept, use, and support AI-powered personalized recommendation services.

At the same time, we recognize that several contextually adapted indicators contain content adjacent to related concepts. Specifically, PR2 includes discomfort associated with intrusive and disruptive recommendations; PR4 includes an avoidance response when recommendations do not match users' interests or needs; PV4 refers to insufficient protection against unauthorized access to personal information; and AW1 reflects willingness to recommend the service to others. These indicators were retained in the primary measurement model because they formed part of the adapted scales administered in the original survey. However, satisfactory reliability, convergent validity, and HTMT values were not treated as sufficient, by themselves, to rule out possible content overlap. Accordingly, supplementary sensitivity analyses were conducted by excluding PR2, PR4, PV4, and AW1 separately and simultaneously to assess whether the substantive structural conclusions depended on these indicators (see Section 4.10 and Table A3 in Appendix A).

The questionnaire included three parts. The first part included screening questions and usage questions such as respondents' experience with AI-powered personalized recommendations, platform type, frequency of usage, and duration of usage. The second part assessed the four focal constructs: perceived privacy invasion [26,37,53], psychological resistance [15,17,54], perceived algorithm transparency [25,55,56], and consumer adoption willingness [4,57]. The third part collected demographic information, including age, gender, region, monthly income, and educational level.

The focal measurement items were phrased in terms of "AI-powered personalized recommendation services" rather than being anchored to one specific named platform. Accordingly, the construct scores should be interpreted as respondents' overall perceptions of AI-powered personalized recommendation services across their recent platform experiences, rather than as evaluations of a single platform. The platform-related usage questions were used to characterize respondents' exposure to different recommendation contexts and were not used to define the referent of the focal latent constructs.

Before the formal survey, a pilot test was conducted with 50 respondents to assess item clarity, wording accuracy, and questionnaire readability. Based on the pilot feedback, minor wording revisions were made where necessary. The pilot test was intended primarily to assess comprehensibility and contextual wording rather than to provide a formal statistical test of construct content validity.

The focal measurement items, their literature sources, and measurement-quality statistics are reported in Table A1, while a concise variable codebook is provided in Table A4 in Appendix A.

3.3. Data Collection

This study was conducted in accordance with the Declaration of Helsinki and received ethical approval from the Human Research Ethics Committee of Walailak University (Approval No. WUEC-25-143-01; approval date: 30 April 2025). Prior to participation, all respondents were presented with an informed consent form explaining the purpose and procedures of the study, potential risks and benefits, the voluntary nature of participation, and their right to withdraw at any time without penalty. Only respondents who provided explicit informed consent were permitted to proceed with the questionnaire.

Data were collected from May to June 2025 through Questionnaire Star, a professional online survey platform in China. The survey invitation was disseminated broadly through WeChat (version 8.0.60), including WeChat Moments, classmate groups, workplace groups, consumer-related groups, and other WeChat groups in which the researchers participated. The researchers also forwarded the invitation to parents and friends, who further shared it through their own WeChat Moments, residential community owner groups, and other WeChat groups in which they participated. These recruitment channels were used to reach adult Internet users with recent experience of AI-powered personalized recommendation services, including those provided by e-commerce, short-video, social/content, and travel-service platforms. Screening questions were used to verify respondents' relevant experience before they commenced the main questionnaire. Respondents who did not meet the screening criteria or did not provide informed consent were not permitted to continue. Because the survey invitation was disseminated and could be further reposted across multiple WeChat-based social networks, the total number of individuals who viewed or were exposed to the invitation could not be reliably determined.

To protect participant privacy, the questionnaire did not request respondents' names, mobile phone numbers, identification numbers, or other direct personal identifiers. A small monetary incentive was provided through WeChat red packets as a token of appreciation for participation. Participation remained voluntary and was not conditional on the disclosure of any personally identifying information.

Several procedural measures were implemented to improve data quality and reduce potential response bias. Respondents were informed that there were no right or wrong answers and were encouraged to answer according to their actual experiences and perceptions. The order of the focal measurement items was randomized to reduce sequence effects, and the survey platform was configured to limit repeated submissions. Responses were excluded if they were incomplete, exhibited obvious straight-lining patterns, had unrealistically short completion times, or contained answers inconsistent with the screening criteria. A total of 600 questionnaire submissions were received during the data-collection period. Following eligibility and data-quality screening, 82 submissions were excluded as invalid or insufficient-quality responses, leaving 518 cases for the final analysis. Thus, 86.33% of the submitted questionnaires were retained as valid analytical cases. Because the total number of individuals exposed to the WeChat invitation could not be determined, this percentage is reported as a valid-case retention rate rather than a conventional invitation-based response rate. Detailed historical counts for the specific reasons underlying the 82 exclusions were not retained and are therefore not reconstructed retrospectively. The anonymized research dataset was stored on the lead researcher's password-protected personal computer and was used solely for academic research purposes. Access to the dataset was restricted to the lead researcher. The anonymized research data will be securely retained for five years following completion of the study and will subsequently be disposed of in accordance with appropriate research-data management practices.

3.4. Data Analysis Methods

This study employed partial least squares structural equation modeling (PLS-SEM) using SmartPLS version 4.1.0.9 to estimate the proposed first-stage moderated mediation model. PLS-SEM was considered appropriate because this study examines multiple latent constructs and simultaneously tests direct, mediating, moderating, and multigroup relationships [48]. In addition, PLS-SEM enables the joint assessment of measurement quality, structural relationships, and out-of-sample predictive performance.

Data analysis proceeded in several stages. First, data screening and descriptive analyses were conducted to examine response quality, sample characteristics, missing values, and the distributions of the focal variables. The reflective measurement model was then evaluated in terms of indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. Specifically, indicator loadings, Cronbach's alpha, rho_A, composite reliability (rho_C), average variance extracted (AVE), and the heterotrait–monotrait ratio (HTMT) were examined in accordance with established PLS-SEM guidelines [48].

Second, the structural model was assessed using inner variance inflation factors (VIFs), coefficients of determination (R^2), effect sizes (f^2), and standardized path coefficients [48]. Statistical inference for the direct, indirect, and interaction effects was based on 10,000 bootstrap resamples using two-tailed significance tests and 95% confidence intervals. The statistical mediating role of psychological resistance (H4) was assessed using the specific indirect effect from the PLS-SEM model. The first-stage moderating role of perceived algorithm transparency (H5) was evaluated through the interaction term between perceived algorithm transparency and perceived privacy invasion (PAT $\times$ PV) predicting psychological resistance.

To directly test the proposed moderated mediation hypothesis (H6), a supplementary conditional process analysis was conducted using PROCESS macro version 4.1 for IBM SPSS Statistics 27, applying Model 7 based on the latent variable scores obtained from the PLS-SEM model. Conditional indirect associations were estimated at low (-1 SD), mean, and high (+1 SD) levels of perceived algorithm transparency using 10,000 bootstrap resamples and 95% bootstrap confidence intervals. The index of moderated mediation was used as the primary inferential test of H6. The first-stage interaction was further probed using simple-slope analysis and the Johnson–Neyman technique to examine how the association between perceived privacy invasion and psychological resistance varied across levels of perceived algorithm transparency.

Third, the model's out-of-sample predictive performance was evaluated using PLSpredict with 10 folds and 10 repetitions following Shmueli et al. [58]. Predictive relevance was assessed using Q^2_predict values, and the prediction errors generated using the PLS-SEM model were compared with those of a linear-model benchmark. Predictive ability was further examined using the cross-validated predictive ability test (CVPAT) following Sharma et al. [59].

Fourth, because all focal constructs were measured using a cross-sectional self-report questionnaire, common method bias was assessed through multiple complementary procedures. Harman's single-factor test was first used as a preliminary diagnostic [60]. This was supplemented by a full-collinearity VIF assessment [61] and the unmeasured latent method construct procedure proposed by Liang et al. [62]. In the latter procedure, each measurement item was modeled with both a substantive component and a common method component, allowing the relative magnitude and significance of substantive and method-related variance to be compared.

Fifth, a targeted Gaussian copula robustness check was conducted for perceived algorithm transparency in the psychological resistance equation. PAT was selected because it serves as the focal moderating construct in the first-stage relationship with psychological resistance. Prior to estimating the copula model, the non-normality requirement of PAT was assessed. A Gaussian copula term for PAT was then included in the psychological resistance equation to examine whether the PAT-related structural estimates were materially altered under this specific adjustment [63,64]. This procedure was treated as a targeted robustness check rather than a comprehensive test of endogeneity across the full model.

Finally, potential age-based heterogeneity was examined across three groups: respondents aged 18–29 years (n = 71), 30–49 years (n = 270), and 50 years and above (n = 177). Before comparing structural coefficients, measurement invariance was assessed using the measurement invariance of composites (MICOM) procedure following Henseler et al. [65]. After establishing at least partial measurement invariance, permutation-based multigroup analysis was conducted to test whether the structural path coefficients differed significantly across the three age groups. Group-specific path estimates were additionally evaluated using 10,000 bootstrap resamples.

4. Results

4.1. Descriptive Statistical Analysis

Table 1 summarizes the demographic characteristics of the 518 valid respondents. The sample was relatively balanced by gender, with males accounting for 51.4% and females for 48.6%. Respondents represented a broad age range: 13.7% were aged 18–29 years, 29.5% were aged 30–39 years, 22.6% were aged 40–49 years, 22.4% were aged 50–59 years, and 11.8% were aged 60 years or above. Thus, respondents aged 50 years or above accounted for 34.2% of the sample. In terms of region, 68.3% of respondents were from urban areas and 31.7% were from rural areas. Monthly income was distributed across all reported categories, with the largest proportions falling between CNY 5001–8000 (21.6%) and CNY 8001–12,000 (20.8%). Respondents also represented diverse educational backgrounds, with bachelor's degree holders comprising the largest group (39.6%).

Respondents also reported substantial experience with AI-powered personalized recommendation services. Regarding the perceived characteristics of such services, 31.7% of respondents indicated that these systems collected relatively large amounts of personal data, while 30.7% emphasized the provision of more accurate recommendations. In terms of usage duration, 44.6% had used AI-powered personalized recommendation services for 3–5 years and 24.7% for 1–3 years. The most commonly reported usage frequency was two to three times per week (37.3%). Regarding daily usage time, 37.3% reported using such services for 30 min to one hour per day, while 29.3% reported one to two hours per day.

Table 1. Demographic characteristics of respondents (N = 518).

Characteristic	Item	Frequency	Percentage
Gender	Male	266	51.4
	Female	252	48.6
Age	18–29 years	71	13.7
	30–39 years	153	29.5
	40–49 years	117	22.6
	50–59 years	116	22.4
	Above 60 years	61	11.8
Region	Urban	354	68.3
	Rural	164	31.7
Average monthly income level	Below 2000	56	10.8
	2001–5000 Yuan	98	18.9
	5001–8000 Yuan	112	21.6
	8001–12,000 Yuan	108	20.8
	12,001–20,000 Yuan	96	18.5
	Above 20,000 Yuan	48	9.3
Highest education level	High school or below	83	16.0
	Associate degree	101	19.5
	Bachelor's degree	205	39.6
	Master's degree	86	16.6
	Doctorate or above	43	8.3

4.2. Assessment of Common Method Bias

Because all focal constructs were measured using the same cross-sectional self-report questionnaire, multiple complementary procedures were employed to assess the potential influence of common method bias (CMB). First, Harman's single-factor test was conducted as a preliminary diagnostic [60]. The first unrotated factor accounted for 47.169% of the total variance, which is below the commonly used 50% benchmark. However, given the limitations of relying solely on Harman's test, additional assessments were conducted.

Second, a full-collinearity assessment was performed using the latent-variable scores of consumer adoption willingness (AW), perceived algorithm transparency (PAT), psychological resistance (PR), and perceived privacy invasion (PV). The resulting full-collinearity VIF values were 1.493 for AW, 1.645 for PAT, 2.000 for PR, and 1.828 for PV. All values were below the conservative threshold of 3.3 [61], providing no indication of problematic full collinearity and suggesting that common method bias was unlikely to materially affect the estimated relationships.

Third, following Liang et al. [62], the unmeasured latent method construct procedure was implemented. Each indicator was modeled with both a substantive component and a common method component. All 16 substantive loadings were statistically significant ($p < 0.001$) and ranged from 0.780 to 0.948, whereas the method-factor loadings ranged from -0.090 to 0.101. Only 2 of the 16 method-factor loadings were statistically significant, while the remaining 14 were nonsignificant. The average substantive variance explained was 0.743, compared with only 0.003 for the average method variance, yielding a substantive-to-method variance ratio of approximately 254:1. Taken together, these results indicate that although some method-related variance may be present, common method bias is unlikely to materially account for the substantive relationships observed in the model. The detailed item-level results of the unmeasured latent method construct assessment are reported in Table 2.

Table 2. Common method bias assessment using the unmeasured latent method construct.

Item	Substantive Loading (R1)	$R1^2$	Method Loading (R2)	$R2^2$	Method p
AW1	0.78	0.608	−0.09	0.008	0.016
AW2	0.929	0.863	0.101	0.01	0.002
AW3	0.792	0.627	−0.034	0.001	0.41
AW4	0.904	0.817	0.019	<0.001	0.556
PAT1	0.879	0.773	0.054	0.003	0.08
PAT2	0.811	0.658	−0.043	0.002	0.21
PAT3	0.803	0.645	−0.037	0.001	0.303
PAT4	0.888	0.789	0.026	0.001	0.415
PR1	0.816	0.666	0.075	0.006	0.059
PR2	0.912	0.832	−0.057	0.003	0.222
PR3	0.82	0.672	0.059	0.003	0.206
PR4	0.948	0.899	−0.077	0.006	0.07
PV1	0.902	0.814	−0.037	0.001	0.399
PV2	0.863	0.745	0.007	<0.001	0.862
PV3	0.86	0.74	0.012	<0.001	0.775
PV4	0.863	0.745	0.017	<0.001	0.671
Mean	—	0.743	—	0.003	—

Note: $R1^2$ represents substantive variance, whereas $R2^2$ represents method variance. All substantive loadings were significant at $p < 0.001$.

4.3. Measurement Model Assessment

The reflective measurement model was assessed in terms of indicator reliability, internal consistency reliability, convergent validity, and discriminant validity. As reported in Appendix A (Table A1), all standardized indicator loadings ranged from 0.825 to 0.884, exceeding the recommended threshold of 0.70. Cronbach's alpha values ranged from 0.867 to 0.897, rho_A values ranged from 0.869 to 0.898, and composite reliability (rho_C) values ranged from 0.909 to 0.928, indicating satisfactory internal consistency reliability. In addition, the average variance extracted (AVE) values ranged from 0.715 to 0.763, exceeding the recommended threshold of 0.50 and supporting convergent validity [48].

Discriminant validity was assessed using the heterotrait–monotrait ratio (HTMT). As shown in Table 3, all HTMT values ranged from 0.396 to 0.673, which is well below the conservative threshold of 0.85 [48]. The highest HTMT value was observed between perceived algorithm transparency and psychological resistance (HTMT = 0.673). These results support the empirical distinctiveness of the four focal constructs and indicate satisfactory discriminant validity. It should be noted, however, that statistical discriminant validity does not by itself establish the absence of conceptual overlap in item content. Because PR2, PR4, PV4, and AW1 contain wording that may be adjacent to discomfort, avoidance, security protection, or advocacy-related responses, respectively, additional indicator-exclusion sensitivity analyses were conducted and are reported in Section 4.10 and Table A3 in Appendix A.

Table 3. Discriminant validity assessment using the HTMT.

Variable	AW	PAT	PR	PV
Consumer Adoption Willingness (AW)				
Perceived Algorithm Transparency (PAT)	0.396			
Psychological Resistance (PR)	0.555	0.673		
Perceived Privacy Invasion (PV)	0.593	0.580	0.660	

Note: HTMT = heterotrait–monotrait ratio. All values are below the conservative threshold of 0.85.

4.4. Structural Model Analysis

After establishing satisfactory reliability and validity of the measurement model, the structural model was evaluated in terms of collinearity, explanatory power, effect sizes, and the statistical significance of the structural relationships. First, inner variance inflation factor (VIF) values were assessed to identify potential collinearity among the predictor constructs. As shown in Table 4, the VIF values ranged from 1.352 to 1.811, indicating that collinearity was not a concern in the structural model [48].

Table 4. Structural model results.

Variable Path Relationship		β	Standard Deviation	T-Value	*p*-Value	95% Confidence Interval	VIF	f^2	Result
Hypothesis	**Path**								
H1	PV → AW	−0.357	0.049	7.330	<0.001	[−0.453, −0.263]	1.542	0.123	Supported
H2	PV → PR	0.279	0.070	3.993	<0.001	[0.142, 0.412]	1.811	0.085	Supported
H3	PR → AW	−0.286	0.048	5.954	<0.001	[−0.379, −0.190]	1.542	0.079	Supported
H4	PAT → PR	−0.391	0.047	8.312	<0.001	[−0.488, −0.304]	1.352	0.224	—
H5	PAT × PV → PR	−0.162	0.047	3.458	0.001	[−0.255, −0.071]	1.480	0.054	Supported

Note: PV = Perceived Privacy Invasion; PR = Psychological Resistance; PAT = Perceived Algorithm Transparency; AW = Consumer Adoption Willingness. R^2(PR) = 0.494; R^2(AW) = 0.330. Bootstrap resamples = 10,000. VIF = variance inflation factor; f^2 = effect size.

The explanatory power of the model was assessed using the coefficient of determination (R^2). The model explained 49.4% of the variance in psychological resistance (PR; R^2 = 0.494) and 33.0% of the variance in consumer adoption willingness (AW; R^2 = 0.330), indicating meaningful explanatory power for both endogenous constructs.

Effect sizes (f^2) were also examined to assess the relative contribution of each predictor to its respective endogenous construct. Perceived algorithm transparency had a medium effect on psychological resistance (f^2 = 0.224), whereas perceived privacy invasion on consumer adoption willingness (f^2 = 0.123), perceived privacy invasion on psychological resistance (f^2 = 0.085), psychological resistance on consumer adoption willingness (f^2 = 0.079), and the interaction between perceived algorithm transparency and perceived privacy invasion on psychological resistance (f^2 = 0.054) exhibited small but nontrivial effect sizes [48].

Statistical inference was based on 10,000 bootstrap resamples using two-tailed tests and 95% confidence intervals. Perceived privacy invasion was significantly and negatively associated with consumer adoption willingness (β = −0.357, t = 7.330, $p < 0.001$, 95% CI [−0.453, −0.263]), supporting H1. Perceived privacy invasion was significantly and positively associated with psychological resistance (β = 0.279, t = 3.993, $p < 0.001$, 95% CI [0.142, 0.412]), supporting H2. Psychological resistance was significantly and negatively associated with consumer adoption willingness (β = −0.286, t = 5.954, $p < 0.001$, 95% CI [−0.379, −0.190]), supporting H3. Perceived algorithm transparency was also negatively associated with psychological resistance (β = −0.391, t = 8.312, $p < 0.001$, 95% CI [−0.488, −0.304]). Finally, the interaction between perceived algorithm transparency and perceived privacy invasion was negative and statistically significant (β = −0.162, t = 3.458, $p = 0.001$, 95% CI [−0.255, −0.071]), supporting H5.

Figure 2 provides a visual summary of the estimated structural model, including the standardized path coefficients, significance levels, and R^2 values of the endogenous constructs. The mediating and moderating mechanisms are examined in greater detail in Sections 4.5 and 4.6, respectively.

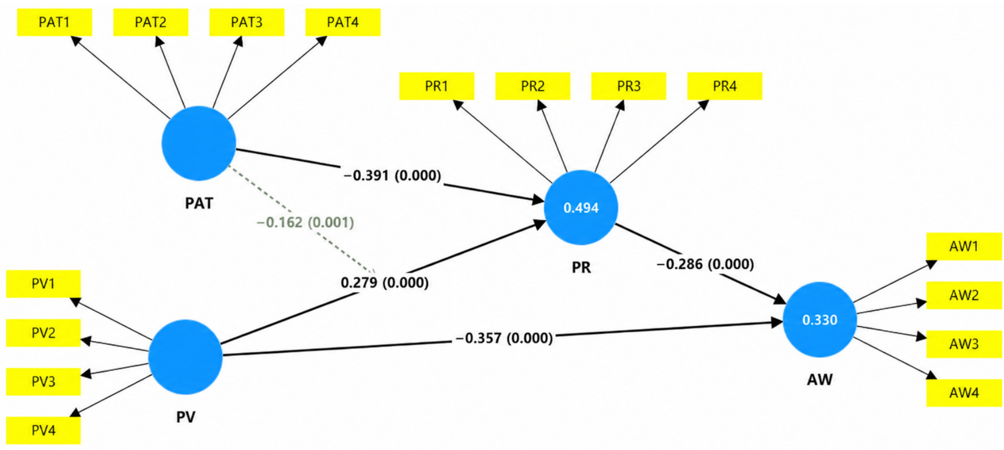

Figure 2. Results of the structural model. Note: Values on the structural paths represent standardized path coefficients, with *p*-values shown in parentheses. Values inside the endogenous constructs represent R^2. Blue circles represent latent constructs, and yellow rectangles represent measurement indicators. The dotted line represents the moderating effect. PV = Perceived Privacy Invasion; PR = Psychological Resistance; PAT = Perceived Algorithm Transparency; AW = Consumer Adoption Willingness.

4.5. Mediation Analysis

The mediating role of psychological resistance in the relationship between perceived privacy invasion and consumer adoption willingness was examined using a bootstrapping procedure with 10,000 resamples. As shown in Table 5, the specific indirect effect of perceived privacy invasion on consumer adoption willingness through psychological resistance was negative and statistically significant (β = −0.080, t = 3.337, $p = 0.001$, 95% CI [−0.130, −0.037]). Because the bootstrap confidence interval did not include zero, the indirect association was statistically significant, providing support for H4.

Table 5. Mediation analysis results.

Effect	Path	β	T-Value	*p*-Value	95% Confidence Interval	Result
Direct effect	PV → AW	−0.357	7.33	<0.001	[−0.453, −0.263]	Significant
Specific indirect effect	PV → PR → AW	−0.080	3.337	0.001	[−0.130, −0.037]	H4 Supported
Total effect	PV → AW	−0.436	9.136	<0.001	—	Significant

At the same time, the direct association between perceived privacy invasion and consumer adoption willingness remained statistically significant after psychological resistance was included in the model (β = −0.357, t = 7.330, $p < 0.001$, 95% CI [−0.453, −0.263]). The total association between perceived privacy invasion and consumer adoption willingness was also statistically significant (β = −0.436, t = 9.136, $p < 0.001$). Taken together, these results indicate that psychological resistance statistically partially mediates the negative association between perceived privacy invasion and consumer adoption willingness. In other words, perceived privacy invasion is associated with lower adoption willingness both directly and indirectly through higher psychological resistance.

4.6. Moderation Analysis

The moderating role of perceived algorithm transparency (PAT) in the relationship between perceived privacy invasion (PV) and psychological resistance (PR) was examined by including the interaction term between PAT and PV in the structural model. Statistical inference was based on 10,000 bootstrap resamples using two-tailed tests and 95% confidence intervals. As reported in Table 4, the interaction between perceived algorithm transparency and perceived privacy invasion was negative and statistically significant (β = −0.162, t = 3.458, *p* = 0.001, 95% CI [−0.255, −0.071]), providing support for H5. The main association between perceived privacy invasion and psychological resistance was positive and statistically significant (β = 0.279, *p* < 0.001), whereas perceived algorithm transparency was negatively associated with psychological resistance (β = −0.391, *p* < 0.001).

To probe the statistically significant interaction in greater detail, a supplementary simple-slope analysis was conducted using the latent variable scores obtained from the PLS-SEM model. The positive association between perceived privacy invasion and psychological resistance was strongest at low PAT (−1 SD; b = 0.4415, SE = 0.0377, t = 11.7141, *p* < 0.001, 95% CI [0.3675, 0.5155]). At the mean level of PAT, the association remained positive and statistically significant (b = 0.2790, SE = 0.0422, t = 6.6106, *p* < 0.001, 95% CI [0.1961, 0.3620]). At high PAT (+1 SD), however, the association became substantially weaker and was no longer statistically significant at the 0.05 level (b = 0.1166, SE = 0.0636, t = 1.8325, *p* = 0.0675, 95% CI [−0.0084, 0.2416]). These results provide inferential support for the buffering role of PAT: as perceived algorithm transparency increases, the positive association between perceived privacy invasion and psychological resistance becomes progressively weaker. This interaction pattern is illustrated in Figure 3.

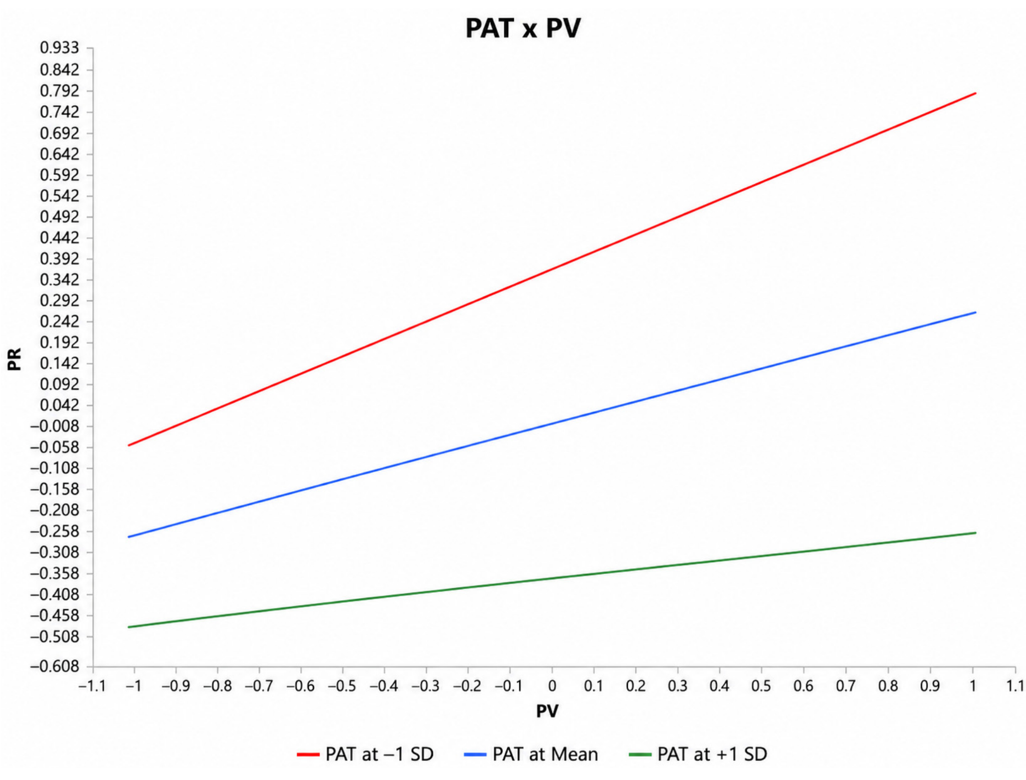

Figure 3. Simple slope plot of the moderating effect of perceived algorithm transparency. Note: The figure illustrates the conditional association between perceived privacy invasion (PV) and psychological resistance (PR) at low (−1 SD), mean, and high (+1 SD) levels of perceived algorithm transparency (PAT).

The Johnson–Neyman analysis provided a more fine-grained assessment of the interaction. The transition point occurred at a standardized PAT value of approximately 0.9613. The positive association between perceived privacy invasion and psychological resistance was statistically significant when PAT was below this value, whereas it was no longer statistically significant above this threshold at the 0.05 level. Approximately 91.31% of the observations fell below this transition point. Thus, the attenuation of the PV–PR association was not limited to the three conventional probing values but was also evident across the observed range of PAT.

Conditional Indirect Effects and Moderated Mediation

To determine whether perceived algorithm transparency also conditioned the indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance, a supplementary conditional process analysis was conducted using PROCESS Model 7 based on the latent variable scores obtained from the PLS-SEM model. The analysis used 10,000 bootstrap resamples and 95% bootstrap confidence intervals. Conditional indirect associations were estimated at low (−1 SD), mean, and high (+1 SD) levels of PAT.

As shown in Table 6, the negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance varied systematically across levels of PAT. At low PAT (−1 SD), the conditional indirect association was statistically significant and relatively strong (b = −0.1262, BootSE = 0.0261, 95% bootstrap CI [−0.1800, −0.0779]). At the mean level of PAT, the indirect association remained statistically significant (b = −0.0797, BootSE = 0.0243, 95% bootstrap CI [−0.1299, −0.0364]). At high PAT (+1 SD), however, the negative indirect association weakened substantially and was no longer statistically significant because the bootstrap confidence interval included zero (b = −0.0333, BootSE = 0.0318, 95% bootstrap CI [−0.0949, 0.0285]).

Table 6. Conditional indirect associations and index of moderated mediation.

PAT Level	Conditional Indirect Association	BootSE	BootLLCI	BootULCI
Low PAT (−1 SD; −1.001)	−0.1262	0.0261	−0.1800	−0.0779
Mean PAT (0.000)	−0.0797	0.0243	−0.1299	−0.0364
High PAT (+1 SD; 1.001)	−0.0333	0.0318	−0.0949	0.0285
Index of moderated mediation	0.0464	0.0161	0.0191	0.0816

Note: Conditional indirect associations were estimated using PROCESS Model 7 with 10,000 bootstrap resamples based on the PLS-SEM latent variable scores. Bootstrap confidence intervals that do not include zero indicate statistical significance. PAT = Perceived Algorithm Transparency.

Most importantly, the index of moderated mediation was positive and statistically different from zero (index = 0.0464, BootSE = 0.0161, 95% bootstrap CI [0.0191, 0.0816]). Because the bootstrap confidence interval excluded zero, the results provide statistical evidence that the indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance varies as a function of perceived algorithm transparency. Specifically, the negative indirect association becomes progressively weaker as PAT increases. These findings therefore support H6 and provide direct evidence for the proposed first-stage moderated mediation mechanism.

These conditional indirect associations should nevertheless be interpreted statistically rather than causally, because the cross-sectional design does not establish temporal ordering among perceived privacy invasion, psychological resistance, and consumer adoption willingness.

4.7. Predictive Assessment

To assess the model's out-of-sample predictive performance, PLSpredict was conducted using 10 folds and 10 repetitions. As reported in Table 7, all Q^2_predict values were greater than zero, ranging from 0.168 to 0.384, indicating predictive relevance for all indicators of consumer adoption willingness (AW) and psychological resistance (PR).

Table 7. PLSpredict results.

Construct	Indicator	Q^2_Predict	PLS-SEM RMSE	LM RMSE	Comparison
AW	AW1	0.225	1.216	1.23	PLS-SEM better
AW	AW2	0.168	1.247	1.242	LM slightly better
AW	AW3	0.207	1.215	1.218	PLS-SEM better
AW	AW4	0.206	1.185	1.185	Equal
PR	PR1	0.384	1.028	1.03	PLS-SEM better
PR	PR2	0.348	1.061	1.046	LM slightly better
PR	PR3	0.379	1.02	1.034	PLS-SEM better
PR	PR4	0.334	1.145	1.156	PLS-SEM better

Note: Q^2_predict values greater than zero indicate predictive relevance relative to the naïve indicator mean benchmark. Lower RMSE values indicate better predictive performance. AW = Consumer Adoption Willingness; PR = Psychological Resistance.

The prediction errors of the PLS-SEM model were further compared with those of a linear-model (LM) benchmark. The PLS-SEM model produced lower RMSE values than the LM benchmark for five of the eight indicators, an identical RMSE for one indicator, and slightly higher RMSE values for two indicators. Taken together, these results indicate moderate out-of-sample predictive power [58].

To further evaluate predictive performance, a cross-validated predictive ability test (CVPAT) was conducted. As shown in Table 8, the PLS-SEM model produced significantly lower prediction loss than the indicator-average (IA) benchmark for both endogenous constructs. For AW, the difference in average loss was −0.374 (t = 5.768, $p < 0.001$), whereas for PR the difference was −0.638 (t = 10.177, $p < 0.001$). At the overall model level, the PLS-SEM loss was 1.306 compared with 1.811 for the IA benchmark, resulting in a significant loss difference of −0.506 (t = 9.745, $p < 0.001$). These findings provide additional evidence that the proposed model possesses meaningful out-of-sample predictive ability [59].

Table 8. Cross-validated predictive ability test (CVPAT) results.

Target Construct	PLS-SEM Loss	IA Benchmark Loss	Loss Difference	t-Value	*p*-Value	Result
AW	1.478	1.851	−0.374	5.768	<0.001	PLS-SEM predicts better
PR	1.133	1.771	−0.638	10.177	<0.001	PLS-SEM predicts better
Overall	1.306	1.811	−0.506	9.745	<0.001	PLS-SEM predicts better

Note: Negative loss differences indicate lower predictive loss for the PLS-SEM model relative to the indicator-average (IA) benchmark. AW = Consumer Adoption Willingness; PR = Psychological Resistance.

4.8. Targeted Gaussian Copula Robustness Check for Perceived Algorithm Transparency

As a targeted robustness check, potential endogeneity involving perceived algorithm transparency (PAT) in the psychological resistance (PR) equation was examined using the Gaussian copula approach. PAT was examined because it serves as the focal moderating construct in the first-stage relationship with PR. This analysis was intended to evaluate whether the PAT-related structural estimates were sensitive to this specific copula adjustment and was not designed as a comprehensive test of endogeneity across the full mediation model. Prior to estimating the copula model, the distributional requirement of the Gaussian copula approach was examined. The construct score of PAT exhibited significant non-normality according to the Cramér–von Mises test ($p < 0.001$), satisfying the distributional prerequisite for applying the Gaussian copula procedure [63,64].

A Gaussian copula term for PAT was subsequently included in the PR equation. As shown in Table 9, the Gaussian copula term was not statistically significant (β = 0.085, t = 0.862, p = 0.389, 95% CI [−0.128, 0.257]). as the confidence interval included zero.

Table 9. Targeted Gaussian Copula Robustness Check for PAT.

Test/Term	β	t-Value	*p*-Value	95% Confidence Interval	Result
Cramér–von Mises test for PAT	—	—	<0.001	—	Non-normality requirement satisfied
GC(PAT) → PR	0.085	0.862	0.389	[−0.128, 0.257]	Not significant

Note: GC(PAT) denotes the Gaussian copula term associated with perceived algorithm transparency. PAT = Perceived Algorithm Transparency; PR = Psychological Resistance.

The PAT-related structural estimates remained broadly similar after inclusion of the Gaussian copula term. In the copula-adjusted model, PAT remained negatively associated with PR (β = −0.485, 95% CI [−0.684, −0.244]), perceived privacy invasion remained positively associated with PR (β = 0.248, 95% CI [0.139, 0.367]), and the interaction between PAT and perceived privacy invasion remained negative (β = −0.155, 95% CI [−0.271, −0.069]). The explained variance in PR also remained essentially unchanged (R^2 = 0.496, compared with 0.494 in the baseline model).

Taken together, this targeted analysis suggests that the PAT-related estimates were not materially changed by the specific Gaussian copula adjustment. However, the analysis does not address possible endogeneity involving other constructs, reciprocal relationships, omitted common antecedents, or temporal ordering within the mediation process. Accordingly, given the cross-sectional observational design, all structural, indirect, and moderated mediation results should be interpreted as statistical associations rather than definitive causal effects.

4.9. Age-Based Measurement Invariance and Multigroup Analysis

To examine potential age-based heterogeneity in the structural relationships, respondents were divided into three categories: 18–29 years (n = 71), 30–49 years (n = 270), and 50 years and above (n = 177). Before comparing structural path coefficients, measurement invariance was assessed using the measurement invariance of composites (MICOM) procedure with 10,000 permutations.

As summarized in Table 10, compositional invariance was established for all four focal constructs—consumer adoption willingness (AW), perceived algorithm transparency (PAT), psychological resistance (PR), and perceived privacy invasion (PV)—across all three pairwise age-group comparisons. Specifically, the original compositional correlations exceeded the corresponding 5% permutation quantiles in each comparison. For the 18–29 versus 30–49 and 18–29 versus 50+ comparisons, no statistically significant differences in composite means or variances were detected, supporting full measurement invariance. For the 30–49 versus 50+ comparison, the composite mean of PV differed significantly between groups (mean difference = 0.226, p = 0.020), whereas the remaining composite-mean comparisons and all composite-variance comparisons were nonsignificant. Accordingly, partial measurement invariance was established for the 30–49 versus 50+ comparison. Because compositional invariance was established for all focal constructs in all three pairwise comparisons, subsequent comparisons of structural path coefficients were considered appropriate. Complete MICOM statistics are reported in Table A2 in Appendix A.

Following the MICOM assessment, permutation-based multigroup analysis was conducted to examine potential differences in structural path coefficients across the three age groups. Pairwise between-group comparisons were based on 10,000 permutations using two-tailed tests at the 0.05 significance level. Group-specific path coefficients were additionally evaluated using 10,000 bootstrap resamples. The results are reported in Table 11.

Table 10. Summary of MICOM results across age groups.

Age-Group Comparison	Step 2: Compositional Invariance	Step 3a: Equality of Composite Means	Step 3b: Equality of Composite Variances	Overall MICOM Result
18–29 vs. 30–49	Established for AW, PAT, PR, and PV	No significant differences	No significant differences	Full invariance
18–29 vs. 50+	Established for AW, PAT, PR, and PV	No significant differences	No significant differences	Full invariance
30–49 vs. 50+	Established for AW, PAT, PR, and PV	PV differed significantly (Δ = 0.226, p = 0.020); others nonsignificant	No significant differences	Partial invariance

Note: MICOM was assessed using 10,000 permutations. Step 2 evaluates compositional invariance, Step 3a evaluates equality of composite means, and Step 3b evaluates equality of composite variances. Full numerical MICOM results, including original compositional correlations, permutation benchmarks, confidence intervals, and permutation p-values, are reported in Table A2 in Appendix A.

Table 11. Age-group structural estimates and pairwise permutation tests.

Structural Path	18–29 β (p)	30–49 β (p)	50+ β (p)	18–29 vs. 30–49 p	18–29 vs. 50+ p	30–49 vs. 50+ p
PAT $\rightarrow$ PR	−0.246 (0.047)	−0.362 (<0.001)	−0.487 (<0.001)	0.451	0.095	0.241
PR $\rightarrow$ AW	−0.336 (0.010)	−0.295 (<0.001)	−0.256 (0.001)	0.811	0.578	0.716
PV $\rightarrow$ AW	−0.278 (0.047)	−0.326 (<0.001)	−0.436 (<0.001)	0.782	0.277	0.311
PV $\rightarrow$ PR	0.462 (0.007)	0.340 (<0.001)	0.086 (0.218)	0.633	0.069	0.081
PAT $\times$ PV $\rightarrow$ PR	−0.140 (0.241)	−0.149 (0.015)	−0.242 (<0.001)	0.955	0.564	0.408

Note: Values in the three age-group columns represent group-specific standardized path coefficients, with bootstrap p-values reported in parentheses. The final three columns report two-tailed permutation p-values for pairwise differences in structural path coefficients based on 10,000 permutations. A between-group difference is considered statistically significant when the corresponding permutation p-value is below 0.05. AW = Consumer Adoption Willingness; PAT = Perceived Algorithm Transparency; PR = Psychological Resistance; PV = Perceived Privacy Invasion.

Although several paths differed in their within-group levels of statistical significance, none of the pairwise differences in structural coefficients reached the 0.05 significance level. For example, the interaction between PAT and PV was not statistically significant among respondents aged 18–29 years ($\beta = -0.140$, $p = 0.241$), but was significant among respondents aged 30–49 years ($\beta = -0.149$, $p = 0.015$) and those aged 50 years and above ($\beta = -0.242$, $p < 0.001$). However, the corresponding between-group permutation tests were nonsignificant for all three pairwise comparisons (p = 0.955, 0.564, and 0.408, respectively). Thus, differences in within-group statistical significance should not be interpreted as evidence of significant between-group differences.

A similar pattern was observed for the PV–PR association. The group-specific coefficient was smaller in the 50+ group ($\beta = 0.086$, $p = 0.218$) than in the 18–29 group ($\beta = 0.462$, $p = 0.007$) and the 30–49 group ($\beta = 0.340$, $p < 0.001$). Nevertheless, none of the corresponding pairwise permutation tests reached the 0.05 significance level (18–29 vs. 30–49: $p = 0.633$; 18–29 vs. 50+: $p = 0.069$; 30–49 vs. 50+: $p = 0.081$). The latter two comparisons were relatively close to the conventional significance threshold and should therefore be interpreted cautiously rather than as evidence that the PV–PR association is equivalent across age groups.

Overall, no statistically significant age-based heterogeneity in the structural path coefficients was detected in the present sample. This finding should not be interpreted as evidence of structural equivalence across age groups. In particular, the relatively small size of the 18–29 subgroup (n = 71), compared with the 30–49 (n = 270) and 50+ (n = 177) groups, may have limited statistical power to detect modest between-group differences. The near-threshold permutation results for the PV–PR association further support a cautious interpretation. Larger and more balanced age-group samples are needed before stronger conclusions regarding age-related structural differences or invariance can be drawn.

4.10. Sensitivity Analysis

Given the possibility that several adapted indicators may contain content adjacent to related constructs, supplementary sensitivity analyses were conducted for PR2, PR4, PV4, and AW1. The structural model was re-estimated after excluding each potentially overlapping indicator separately and after excluding all four indicators simultaneously. As reported in Table A3 in Appendix A, the signs and statistical significance of all focal structural associations remained unchanged across the alternative specifications. In the most restrictive specification, in which PR2, PR4, PV4, and AW1 were simultaneously excluded, the associations of PV with AW (β = −0.343, $p < 0.001$), PV with PR (β = 0.247, $p < 0.001$), PR with AW (β = −0.276, $p < 0.001$), and PAT with PR (β = −0.385, $p < 0.001$) remained statistically significant. The PAT × PV interaction also remained significant (β = −0.164, $p = 0.001$), as did the specific indirect association of PV with AW through PR (β = −0.068, $p = 0.003$).

As an additional sensitivity check of the moderated mediation result, PROCESS Model 7 was re-estimated using latent variable scores from the reduced four-indicator-exclusion model. The index of moderated mediation remained statistically significant (index = 0.0451, BootSE = 0.0156, 95% bootstrap CI [0.0187, 0.0789]). The conditional indirect association was significant at low PAT (b = −0.1131, 95% bootstrap CI [−0.1636, −0.0662]) and at the mean level of PAT (b = −0.0680, 95% bootstrap CI [−0.1146, −0.0270]), but not at high PAT (b = −0.0228, 95% bootstrap CI [−0.0815, 0.0369]). Thus, the principal structural and moderated mediation findings were not dependent on the potentially overlapping indicators identified above.

5. Discussion

5.1. Research Findings

The empirical results generally support the proposed first-stage moderated mediation framework. Perceived privacy invasion was negatively associated with consumer adoption willingness and positively associated with psychological resistance, whereas psychological resistance was negatively associated with consumer adoption willingness. The mediation analysis further showed that psychological resistance statistically partially mediated the negative association between perceived privacy invasion and consumer adoption willingness, supporting H4. Perceived algorithm transparency significantly moderated the association between perceived privacy invasion and psychological resistance, such that the positive PV–PR association became less pronounced at higher levels of PAT, supporting H5. Importantly, the supplementary conditional process analysis further showed that the negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance became progressively weaker as PAT increased. The statistically significant index of moderated mediation provided direct support for H6.

The additional analyses provided complementary evidence regarding the predictive performance and robustness of the findings. PLSpredict and CVPAT indicated meaningful out-of-sample predictive ability. The targeted Gaussian copula robustness check further indicated that the PAT-related structural estimates were not materially altered by the specific copula adjustment. This result is interpreted narrowly and does not rule out other forms of endogeneity or establish causal direction. Indicator-exclusion sensitivity analyses further showed that the focal structural and moderated mediation findings did not depend on PR2, PR4, PV4, or AW1. Finally, the age-based multigroup analysis showed that none of the pairwise differences in structural path coefficients reached statistical significance across the 18–29, 30–49, and 50+ age groups. Accordingly, no statistically significant age-based heterogeneity was detected in the present sample; however, this finding should not be interpreted as evidence of structural equivalence across age groups.

5.2. Interpretation of Findings

5.2.1. The Relationship Between Perceived Privacy Invasion, Psychological Resistance, and Consumer Adoption Willingness

The present study shows that perceived privacy invasion is significantly and negatively associated with consumer adoption willingness. This finding suggests that consumer responses to AI-powered personalized recommendations depend not only on recommendation quality and relevance, but also on how users interpret the privacy implications of the underlying data practices. When personalization is perceived as excessive, covert, or disproportionate, users may become less willing to accept, rely on, or continue using the recommendation service [15,66]. These findings are consistent with prior research showing that privacy-related perceptions can shape consumers' responses to personalized and AI-enabled recommendation environments.

Perceived privacy invasion was also positively associated with psychological resistance. This finding extends the discussion beyond general privacy concern by highlighting a motivational response associated with perceived boundary violations. Privacy concern typically reflects users' cognitive evaluation of potential privacy risks, whereas psychological resistance reflects a stronger sense of defensiveness, discomfort, or opposition when users perceive that their autonomy or control is being threatened. Accordingly, users who perceive stronger privacy invasion may also report stronger psychological resistance toward AI-powered recommendation systems [37,40].

From the perspective of psychological reactance theory, this distinction is theoretically meaningful. Privacy-related responses may involve more than a rational comparison of personalization benefits and privacy costs. When recommendation practices are perceived as intrusive or controlling, users may also experience defensiveness, discomfort, and reluctance to be guided by the system [54,67]. The present results are therefore consistent with the view that privacy-related perceptions in AI recommendation environments can be accompanied by autonomy-related motivational responses.

Psychological resistance was, in turn, negatively associated with consumer adoption willingness. This suggests that resistance is not merely an incidental emotional response but is meaningfully related to users' willingness to accept AI-powered recommendations. Similar patterns have been reported in other AI-mediated settings, where intrusive or controlling interactions are associated with avoidance, disengagement, or less favorable behavioral responses even when the underlying AI system may be technically capable [30].

The mediation analysis provides further insight into this relationship. Psychological resistance statistically partially mediated the negative association between perceived privacy invasion and consumer adoption willingness. Specifically, perceived privacy invasion was associated with lower adoption willingness both directly and indirectly through higher psychological resistance. The significant indirect association indicates that psychological resistance represents one motivational pathway linking privacy-related perceptions with adoption willingness, while the remaining significant direct association suggests that other psychological or evaluative processes may also be involved. This interpretation is consistent with prior research suggesting that privacy-related perceptions can influence responses to personalized technologies through intervening psychological and emotional processes [15,16].

These findings also qualify the common assumption that greater personalization necessarily produces more favorable consumer responses. Although personalization can improve relevance and convenience, highly personalized outputs may also signal extensive tracking or hidden inference when users do not understand or accept the underlying data practices. Under such conditions, greater personalization may be accompanied by stronger perceptions of intrusiveness rather than greater perceived value. Recent research on AI-enabled advertising and personalization similarly suggests that highly personalized outputs do not uniformly generate more favorable responses and may be associated with lower effectiveness when they are perceived as intrusive or manipulative [68–70].

Overall, the findings highlight perceived privacy invasion as one specific privacy-related perception that is relevant to consumer responses to AI-powered recommendations. Perceived privacy invasion is associated not only with lower consumer adoption willingness but also with greater psychological resistance, while psychological resistance statistically accounts for part of the negative association between privacy invasion and adoption willingness. This provides a more specific account of the motivational dimension of consumers' privacy-related responses to AI-powered personalized recommendation systems. Because general privacy concern was not measured separately, these findings should not be interpreted as demonstrating empirical discriminant validity between perceived privacy invasion and broader privacy concern.

5.2.2. Discussing the Moderating Role of Perceived Algorithm Transparency

The findings further show that perceived algorithm transparency significantly moderates the positive association between perceived privacy invasion and psychological resistance, supporting H5. Specifically, the association between perceived privacy invasion and psychological resistance becomes weaker as perceived algorithm transparency increases. The simple-slope analysis further showed that this positive association was statistically significant at low and mean levels of PAT but was no longer statistically significant at a high level of PAT. These finding is consistent with prior research suggesting that perceived transparency and explainability can improve users' understanding of algorithmic systems and reduce uncertainty surrounding recommendation logic and data use [25,56].

These findings extend recent JTAER research showing that transparency shapes consumer evaluations and trade-offs in AI-enabled e-commerce settings [43,71]. The present study further suggests that perceived algorithm transparency may operate as a user-level perceptual boundary condition in the privacy invasion–resistance relationship. When users perceive that they can understand why recommendations are generated, what information is used, and how explanations can be obtained, privacy-invasive experiences may be less strongly associated with defensiveness and psychological resistance. In this sense, PAT can be understood as a perceptual resistance-buffering condition, rather than as an objective characteristic of the platform itself [31,32].

Beyond this first-stage moderating effect, the conditional indirect-effect analysis provides support for H6. The negative indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance was strongest when PAT was low, weaker at the mean level of PAT, and no longer statistically significant at high PAT. More importantly, the statistically significant index of moderated mediation indicates that the magnitude of this indirect association systematically varied as a function of perceived algorithm transparency. Thus, PAT conditions not only the first-stage association between perceived privacy invasion and psychological resistance, as proposed in H5, but also the broader indirect privacy invasion–resistance–adoption association, as proposed in H6.

This moderated mediation finding extends prior transparency–acceptance research in an important way. Existing studies have commonly examined transparency as a direct antecedent of trust, perceived legitimacy, or acceptance. The present findings instead suggest that perceived transparency can alter the strength of a negative psychological pathway statistically linking perceived privacy invasion to adoption willingness through psychological resistance. In this sense, PAT operates as a perceptual buffering condition within the privacy-related inhibition pathway rather than merely as an independent positive predictor of acceptance.

This interpretation is particularly relevant in AI-powered recommendation environments, where recommendation processes may appear opaque to users. Users typically observe the personalized output but may have a limited understanding of how the system arrived at that output, what information was used, or why a particular recommendation was presented. Under such conditions, greater perceived transparency may provide interpretive cues that make the recommendation process more understandable and reduce uncertainty surrounding algorithmic personalization [42,72].

At the same time, the results should not be interpreted as suggesting that perceived transparency eliminates privacy concerns. The direct negative association between perceived privacy invasion and consumer adoption willingness remained statistically significant. Thus, perceived algorithm transparency appears to attenuate one psychological pathway—namely, the association between privacy invasion and resistance—but does not fully offset the negative association between privacy invasion and adoption willingness. This finding supports a more conditional view of transparency and suggests that transparency and privacy protection should not be treated as substitutes [32,71].

The results also highlight the importance of distinguishing perceived algorithm transparency from purely technical transparency. The construct examined in this study reflects users' subjective perceptions that recommendation logic, data use, and explanations are understandable and accessible. Therefore, the findings do not demonstrate that objective platform transparency or governance quality directly reduces psychological resistance. Rather, they indicate that users who perceive greater transparency show a weaker association between perceived privacy invasion and psychological resistance. This interpretation is consistent with recent research emphasizing the importance of algorithm awareness and user understanding in shaping responses to personalized recommendation systems [71,72].

Overall, the findings support a conditional perspective on perceived algorithm transparency. PAT is important not because transparency necessarily produces uniformly positive responses to AI systems, but because users' perceived understanding of recommendation processes may provide interpretive resources when privacy-related concerns arise. Accordingly, PAT is better conceptualized in the present study as a user-level perceptual boundary condition than as an objective platform-level governance mechanism.

5.2.3. Age-Based Heterogeneity in the Structural Relationships

The age-based multigroup analysis provides a more cautious picture than would be suggested by simply comparing the statistical significance of coefficients within individual age groups. Respondents were divided into three groups—18–29, 30–49, and 50 years and above—and measurement invariance was established at least partially across all pairwise comparisons. The subsequent permutation-based multigroup analysis showed that none of the five structural relationships differed significantly across age groups.

Some descriptive variation was nevertheless observed. For example, the positive association between perceived privacy invasion and psychological resistance was statistically significant among respondents aged 18–29 and 30–49, but not among respondents aged 50 and above. Similarly, the interaction between perceived algorithm transparency and perceived privacy invasion was statistically significant in the 30–49 and 50+ groups but not in the 18–29 group. However, these differences in within-group significance should not be interpreted as evidence of significant between-group differences, because the corresponding permutation tests were nonsignificant.

The permutation-based multigroup analysis did not detect statistically significant between-group differences in the five structural relationships examined. This finding indicates an absence of detected age-based heterogeneity in the present sample rather than evidence that the structural relationships are equivalent across age categories. Within the limits of the present sample, the results do not provide statistical evidence that the moderating association involving PAT differs across the three age categories. Prior research has similarly emphasized that users' responses to AI systems may depend on more proximal perceptual and cognitive factors, including perceived transparency and algorithm awareness [31,56,71,72].

At the same time, the near-significant pairwise differences observed for the PV–PR relationship warrant cautious attention rather than substantive claims. The comparisons between the 18–29 and 50+ groups and between the 30–49 and 50+ groups yielded permutation p-values of 0.069 and 0.081, respectively. Because these values exceed the conventional 0.05 threshold, the present study does not treat them as evidence of age-based heterogeneity. The relatively small size of the 18–29 subgroup (n = 71) may also have limited statistical power to detect modest between-group differences. Future research with larger and more balanced subgroup samples may examine whether more proximal characteristics—such as algorithm literacy, privacy sensitivity, perceived control, prior AI experience, or digital competence—better explain individual variation in privacy-related responses [37,40,42,66,72,73].

The absence of statistically significant age-group differences should also be interpreted in light of prior technology-adoption research showing that generational variation may reflect differences in motivational factors and consumption values rather than chronological age alone [44]. Thus, the present age categories may not capture the more proximal psychological and value-based characteristics through which age-related differences in technology adoption emerge. Future research could therefore combine chronological age with variables such as digital experience, technology readiness, consumption values, or AI familiarity to provide a more theoretically informative assessment of user heterogeneity.

Overall, the present findings support a cautious interpretation of age-related heterogeneity. Chronological age alone did not produce statistically significant differences in the focal structural relationships, but this does not imply that age-related variation is absent or that age groups are structurally equivalent.

6. Conclusions

This study examined the relationships between perceived privacy invasion, psychological resistance, perceived algorithm transparency, and consumer adoption willingness in the context of AI-powered personalized recommendations. Drawing on the privacy-cost perspective of privacy calculus theory and psychological reactance theory, this study proposed and tested a first-stage moderated mediation model using survey data from 518 Chinese adult Internet users with recent experience of AI-powered personalized recommendation services.

The findings show that perceived privacy invasion is negatively associated with consumer adoption willingness and positively associated with psychological resistance. Psychological resistance, in turn, is negatively associated with adoption willingness and statistically partially mediates the relationship between perceived privacy invasion and consumer adoption willingness. In addition, perceived algorithm transparency moderates the positive association between perceived privacy invasion and psychological resistance, such that this association becomes less pronounced at higher levels of perceived algorithm transparency. The supplementary conditional process analysis further showed that PAT conditioned the indirect association between perceived privacy invasion and consumer adoption willingness through psychological resistance. Specifically, the negative indirect association became progressively weaker as PAT increased, as indicated by a statistically significant index of moderated mediation (index = 0.0464, 95% bootstrap CI [0.0191, 0.0816]).

Additional analyses provide further support for the robustness of the proposed model. The model demonstrated meaningful out-of-sample predictive ability, while a targeted Gaussian copula robustness check indicated that the PAT-related estimates were not materially altered by the specific copula adjustment. Age-based multigroup analysis detected no statistically significant pairwise differences in the structural path coefficients across respondents aged 18–29, 30–49, and 50 years and above. This finding is interpreted as an absence of detected age-based heterogeneity rather than evidence of structural equivalence across age groups. Indicator-exclusion sensitivity analyses also showed that the focal structural and moderated mediation findings were not dependent on the potentially overlapping indicators identified in the measurement model.

Overall, this study highlights that consumer responses to AI-powered personalized recommendations are associated not only with the perceived usefulness or relevance of personalization but also with how users interpret the privacy implications and comprehensibility of algorithmic recommendation processes. By identifying psychological resistance as a motivational pathway and perceived algorithm transparency as a user-level perceptual boundary condition, this study provides a more nuanced account of the statistical pathway associated with lower willingness to adopt AI-powered recommendations when privacy-invasive personalization is experienced.

6.1. Theoretical Contributions

This study makes several theoretical contributions to the literature on AI-powered personalized recommendation, privacy, and consumer adoption.

First, the study extends research on AI-powered personalized recommendations by shifting attention from predominantly value-enhancing mechanisms to a privacy-related inhibition pathway. Prior studies have largely emphasized recommendation relevance, efficiency, trust, satisfaction, and engagement. In contrast, the present findings show that perceived privacy invasion is negatively associated with consumer adoption willingness, highlighting an important cost-related pathway in AI-enabled personalization. This provides a more balanced account of AI recommendation systems as technologies capable of generating both perceived value and negative privacy-related responses.

Second, the study contributes to privacy research by focusing on perceived privacy invasion as an immediate perception that acceptable personal boundaries have been crossed and by linking this perception to psychological resistance. This differs conceptually from broader privacy concern, which typically refers to a more general evaluation of potential privacy risks. The present findings show that perceived privacy invasion is positively associated with an autonomy-related motivational response and is indirectly associated with adoption willingness through psychological resistance. Importantly, because general privacy concern was not included as a separate measured construct, the present study does not claim to empirically establish discriminant validity between perceived privacy invasion and general privacy concern. Rather, its contribution lies in specifying and testing the motivational pathway associated with perceived boundary-crossing experiences in AI-powered recommendation contexts.

Third, the study extends psychological reactance theory to AI-powered personalized recommendation contexts by identifying psychological resistance as a statistical mediating pathway linking perceived privacy invasion and consumer adoption willingness. The significant indirect association through psychological resistance suggests that users' privacy-related perceptions are associated with adoption willingness partly through an autonomy-related motivational response. This contributes to understanding why consumers may resist algorithmic recommendations even when such systems are functionally useful or accurate.

Fourth, this study contributes to research on algorithm transparency by conceptualizing PAT as a user-level perceptual boundary condition. The significant first-stage interaction shows that the positive association between perceived privacy invasion and psychological resistance becomes less pronounced at higher levels of PAT. More importantly, the significant index of moderated mediation indicates that PAT also conditions the broader indirect privacy invasion–resistance–adoption association. This extends transparency research beyond its commonly examined direct associations with trust and acceptance by showing that perceived transparency can alter the strength of a privacy-related psychological pathway. In addition, because general privacy concern was not measured as a separate construct, the conceptual distinction between perceived privacy invasion and broader privacy concern could not be empirically tested in the present study. Future research could include both constructs simultaneously to assess their empirical distinctiveness and potentially different psychological consequences.

Fifth, the study contributes by examining potential age-based heterogeneity in the proposed structural relationships using measurement invariance assessment and permutation-based multigroup analysis. No statistically significant differences in the focal structural paths were detected across the 18–29, 30–49, and 50+ groups. These findings should be interpreted as an absence of detected age-based heterogeneity in the present sample rather than as evidence of structural equivalence across age categories.

Overall, this study integrates the privacy-cost perspective of privacy calculus theory with psychological reactance theory and perceived algorithm transparency to provide a more nuanced explanation of consumer responses to AI-powered personalized recommendations. By identifying both a motivational pathway through psychological resistance and a perceptual boundary condition through PAT, the study clarifies how privacy-related perceptions are associated with lower adoption willingness and under what perceptual conditions these negative responses may be attenuated.

6.2. Managerial Implications

The findings offer several practical implications for digital platform operators, e-commerce firms, and service providers that deploy AI-powered personalized recommendation systems.

First, firms should avoid treating greater personalization as an unconditional route to higher consumer acceptance. The negative association between perceived privacy invasion and adoption willingness suggests that recommendation accuracy and relevance should be balanced against users' privacy boundaries. Platforms should therefore minimize unnecessary data collection, avoid excessive cross-context tracking, and ensure that the degree of personalization is proportionate to the service being provided. Recommendation practices that appear overly precise or based on information that users do not expect the platform to possess may increase perceptions of privacy intrusion and undermine the willingness to use the service.

Second, platform managers should pay attention not only to privacy concerns in a regulatory or informational sense, but also to the psychological resistance that may accompany privacy-invasive experiences. The mediation results suggest that users who perceive stronger privacy invasion are also more likely to report defensiveness, discomfort, and resistance toward the recommendation process. Firms should therefore provide meaningful user control over personalization, such as the ability to modify recommendation preferences, disable specific forms of personalization, reset recommendation histories, or restrict the use of particular categories of personal data. Such controls may help reduce the perception that users are being passively monitored or manipulated by the recommendation system.

Third, firms should improve the perceived transparency of AI recommendation systems by providing explanations that are understandable from the user's perspective. Rather than relying primarily on highly technical descriptions of algorithmic architecture, platforms can offer concise explanations of why particular content is recommended, what types of data contributed to the recommendation, and how users can influence future recommendations. The moderating result suggests that when users perceive the recommendation process as more understandable and explainable, the positive association between privacy invasion and psychological resistance is less pronounced. The conditional indirect-effect results further suggest that greater perceived transparency may reduce the extent to which privacy-invasive experiences are statistically associated with lower adoption willingness through psychological resistance.

However, perceived transparency should not be treated as a substitute for substantive privacy protection. The direct negative association between perceived privacy invasion and adoption willingness remained significant even after psychological resistance and perceived algorithm transparency were considered. Consequently, firms should not assume that providing explanations alone can compensate for data practices that users regard as intrusive. A more sustainable strategy is to combine understandable explanations with privacy-by-design practices, data minimization, meaningful consent, and accessible user controls.

Finally, no statistically significant age-based heterogeneity was detected in the structural relationships examined in the present sample. This finding should not be interpreted as evidence of structural equivalence across age categories. Accordingly, platforms should not rely solely on chronological age when designing privacy and transparency interventions. Instead, more individualized factors—such as users' algorithm literacy, privacy sensitivity, prior AI experience, and desired level of control—may provide more useful bases for tailoring recommendation explanations and privacy settings.

6.3. Research Limitations and Future Prospects

Despite its contributions, this study has several limitations that provide opportunities for future research.

First, the study employed a cross-sectional survey design, which limits strong causal inference regarding the proposed relationships. Although the theoretical framework specifies directional relationships between perceived privacy invasion, psychological resistance, perceived algorithm transparency, and consumer adoption willingness, all focal variables were measured at a single point in time. The targeted Gaussian copula analysis indicated that the PAT-related structural estimates were not materially altered by this specific copula adjustment; however, this result should not be interpreted as evidence that endogeneity is absent from the broader model or as establishing causal direction. Future studies could employ longitudinal, experimental, or panel designs to examine how privacy-related perceptions and psychological resistance develop over time and to provide stronger evidence regarding temporal and causal ordering. The statistically significant moderated mediation pattern should therefore be interpreted as a conditional indirect association rather than evidence of a causal process. In particular, the cross-sectional design cannot exclude plausible reverse relationships, such as the possibility that users with stronger psychological resistance retrospectively perceive personalized recommendation practices as more privacy-invasive, nor can it rule out omitted common antecedents that may jointly influence privacy perceptions, resistance, and adoption willingness.

Second, the data were collected from adult Internet users in China. China provides a relevant setting because AI-powered personalized recommendation services are widely embedded in e-commerce, short-video, social/content, and travel-service platforms. Nevertheless, privacy norms, regulatory environments, technology expectations, and responses to algorithmic personalization may differ across countries and cultural contexts. Future research should therefore replicate the proposed model across different institutional and cultural settings to evaluate its cross-cultural generalizability.

Third, all focal constructs were measured using self-reported perceptual data. Multiple complementary diagnostics—including Harman's single-factor test, full-collinearity VIF assessment, and the unmeasured latent method construct procedure—suggested that common method bias was unlikely to materially account for the reported relationships. Nevertheless, self-reported adoption willingness may not fully correspond to actual behavior. Future studies could combine survey measures with behavioral indicators such as clickstream data, recommendation acceptance records, platform usage logs, or experimentally observed choices. In addition, the focal measurement items were not anchored to a single named digital platform. The construct scores therefore reflect respondents' overall perceptions across their recent experiences with AI-powered personalized recommendation services. Although this approach is consistent with the cross-platform focus of the study, it does not allow the analysis to isolate platform-specific differences in privacy invasion, psychological resistance, transparency perceptions, or adoption willingness. Future research could employ platform-specific referents or compare otherwise equivalent models across e-commerce, short-video, social/content, and travel-service platforms.

Fourth, although the indicator-exclusion sensitivity analyses showed that the substantive findings were robust to the removal of PR2, PR4, PV4, and AW1, the contextual adaptation of several items may still involve conceptual content adjacent to discomfort, avoidance, security protection, or advocacy-related responses. Future research could refine these measures further and conduct dedicated content-validity assessments before data collection.

Fifth, the proposed model focuses on one mediating mechanism, psychological resistance, and one moderating condition, perceived algorithm transparency. Although these constructs were theoretically central to the present study, other psychological and perceptual mechanisms may also explain consumer responses to privacy-invasive personalization. Future research could examine additional mediators such as trust, perceived manipulation, perceived control, or perceived fairness, as well as other boundary conditions such as algorithm literacy, AI experience, privacy sensitivity, or user empowerment.

Sixth, the age-based multigroup analysis found no statistically significant differences in the structural relationships across the 18–29, 30–49, and 50+ groups. Although some subgroup coefficients varied descriptively, these differences were not statistically supported by the permutation tests. Thus, chronological age may be too broad a proxy for the cognitive, experiential, and privacy-related characteristics that shape responses to AI-powered recommendations. Future research could examine more proximal individual-level characteristics, including algorithm literacy, digital competence, privacy sensitivity, perceived control, and prior experience with AI systems.

Seventh, the present study examined AI-powered personalized recommendation services across multiple digital platform contexts in order to capture the general privacy–resistance–adoption mechanism. However, recommendation environments may differ across e-commerce, short-video, social/content, and travel-service platforms in terms of data intensity, recommendation purpose, user expectations, and perceived intrusiveness. Future research could employ platform-specific samples or sufficiently large subsamples to test whether the structural relationships identified in this study vary systematically across platform types.

Finally, perceived algorithm transparency in this study was measured as a user-level perceptual construct. The findings therefore should not be interpreted as evidence regarding the objective transparency, technical explainability, or governance quality of the underlying platforms. Future research could distinguish between objective transparency interventions and users' subjective perceptions of transparency, and experimentally examine whether changes in disclosure format, explanation depth, data-use visibility, or user-control features alter perceived transparency and subsequent privacy-related responses.

Overall, these limitations suggest that future research should extend the present framework through stronger causal designs, behavioral data, cross-cultural replication, platform-specific comparisons, and more fine-grained individual-difference measures. Such extensions would help clarify when and for whom privacy-related perceptions shape responses to AI-powered personalized recommendation systems.

7. Declaration of Generative AI Use

During the preparation and revision of this manuscript, the authors used ChatGPT (OpenAI; GPT-5.6 Sol) to assist with language refinement and structural editing. All AI-assisted outputs were critically reviewed, verified, and revised by the authors, who take full responsibility for the final content of the manuscript.

Author Contributions: Conceptualization, X.Z., S.P. and P.P.; methodology, X.Z., S.P. and P.P.; software, X.Z.; validation, X.Z.; formal analysis, X.Z. and S.P.; investigation, X.Z.; resources, S.P.; data curation, X.Z.; writing—original draft preparation, X.Z., S.P., P.P. and Y.E.; writing—review and editing, X.Z., S.P., P.P. and Y.E.; visualization, X.Z.; supervision, S.P. and P.P.; project administration, X.Z. and S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study was conducted in accordance with the Declaration of Helsinki and was approved by the Ethics Committee in Human Research Walailak University (approval number: WUEC-25-143-01; date of approval: 30 April 2025).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The focal measurement items, variable codebook, and key robustness-analysis results are provided in Appendix A. The anonymized analytical data and additional analysis materials are available from the corresponding author upon reasonable request, subject to applicable ethical, privacy, and institutional requirements. Participant-level data are not publicly deposited because they are managed under the research team's data-protection procedures.

Acknowledgments: The authors sincerely thank all respondents who participated in this study. This project was conducted within the Reinventing Project for Enhancing Thai Universities into the International Education, the Ministry of Higher Education, Science, Research, and Innovation. The authors also acknowledge the support of the Faculty Development Plan of Guangzhou Huashang Vocational College.

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

Appendix A

Table A1. Measurement items and reliability and convergent validity assessment.

Item No	Construct and Measurement Item	Factor Loading	Cronbach's Alpha	rho_A	Composite Reliability (rho_C)	AVE	Literature Source
Perceived Privacy Invasion (PV)							
PV1	I feel that my personal information is monitored, searched, recorded, or stored by AI personalized recommendation services without my permission.	0.866	0.895	0.896	0.927	0.76	[26,37,53]
PV2	I feel that my personal information is shared with third parties by AI personalized recommendation services without my permission.	0.87					
PV3	I believe that the collection of my personal information by AI personalized recommendation services creates numerous potential privacy issues.	0.871					
PV4	I believe that relevant companies or organizations do not take sufficient measures to prevent unauthorized access to personal information by AI personalized recommendation services.	0.881					
Psychological Resistance (PR)							
PR1	I feel annoyed when AI personalized recommendation services overly restrict my browsing freedom by forcing recommendations.	0.884	0.897	0.898	0.928	0.763	[15,17,54]
PR2	Overall, I find AI personalized recommendation services invasive and disruptive, which makes me uncomfortable.	0.858					
PR3	The excessive personalization of AI personalized recommendation systems makes me feel manipulated, which reduces my trust in the recommended content.	0.874					
PR4	When the AI-recommended content does not match my interests or needs, I feel repelled and tend to avoid using the service.	0.878					

Table A1. *Cont.*

Item No	Construct and Measurement Item	Factor Loading	Cronbach's Alpha	rho_A	Composite Reliability (rho_C)	AVE	Literature Source
Perceived Algorithm Transparency (PAT)							
PAT1	I find the way the AI personalized recommendation algorithm works to be clear to me.	0.83	0.867	0.869	0.909	0.715	[25,55,56]
PAT2	I understand how the AI personalized recommendation algorithm generates recommended content.	0.849					
PAT3	I can know what data the AI recommendation system uses to generate recommendations.	0.835					
PAT4	When I have doubts about the recommendation results, I can obtain clear explanations to help me understand.	0.868					
Consumer Adoption Willingness (AW)							
AW1	I would recommend others to use AI personalized recommendation services.	0.858	0.874	0.878	0.914	0.726	[4,57]
AW2	I am willing to browse products or information recommended by AI personalized recommendation services.	0.84					
AW3	I am willing to purchase items or accept information recommended by AI personalized recommendation services.	0.825					
AW4	Overall, I am willing to browse with the assistance of AI personalized recommendation services.	0.884					

Table A2. Full MICOM Results Across Age-Group Comparisons.

Construct	Orig. Corr.	Perm. Mean	5%	Step2 *p*	Mean Diff.	Mean CI	Mean *p*	Var. Diff.	Var. CI	Var. *p*
18–29 vs. 30–49										
AW	1	0.998	0.996	0.849	0.139	[−0.266, 0.263]	0.298	−0.125	[−0.321, 0.237]	0.359
PAT	1	0.999	0.997	0.75	0.097	[−0.268, 0.256]	0.47	−0.088	[−0.337, 0.255]	0.544
PR	1	1	0.999	0.578	−0.183	[−0.258, 0.267]	0.165	−0.132	[−0.363, 0.274]	0.408
PV	0.999	1	0.999	0.269	−0.074	[−0.259, 0.262]	0.58	−0.089	[−0.386, 0.286]	0.592
18–29 vs. 50+										
AW	0.999	0.999	0.996	0.434	0.114	[−0.283, 0.276]	0.419	−0.161	[−0.325, 0.255]	0.273
PAT	1	0.999	0.997	0.805	0.104	[−0.278, 0.274]	0.462	−0.101	[−0.332, 0.259]	0.499
PR	0.999	1	0.999	0.123	−0.115	[−0.274, 0.282]	0.424	−0.317	[−0.387, 0.298]	0.068
PV	1	0.999	0.998	0.807	0.156	[−0.265, 0.284]	0.273	−0.008	[−0.466, 0.369]	0.968

Table A2. *Cont.*

Construct	Orig. Corr.	Perm. Mean	5%	Step2 *p*	Mean Diff.	Mean CI	Mean *p*	Var. Diff.	Var. CI	Var. *p*
30–49 vs. 50+										
AW	1	0.999	0.998	0.662	−0.025	[−0.191, 0.187]	0.803	−0.030	[−0.179, 0.198]	0.747
PAT	1	1	0.999	0.642	0.007	[−0.187, 0.190]	0.94	−0.013	[−0.182, 0.196]	0.89
PR	1	1	1	0.304	0.054	[−0.191, 0.192]	0.579	−0.185	[−0.201, 0.220]	0.083
PV	1	1	0.999	0.334	0.226	[−0.188, 0.191]	0.02	0.084	[−0.238, 0.260]	0.511

Note: MICOM results are based on 10,000 permutations. Step 2 assesses compositional invariance. Step 3a assesses equality of composite means, and Step 3b assesses equality of composite variances. AW = Consumer Adoption Willingness; PAT = Perceived Algorithm Transparency; PR = Psychological Resistance; PV = Perceived Privacy Invasion.

Table A3. Sensitivity Analyses Excluding Potentially Overlapping Indicators.

Specification	PV → AW	PV → PR	PR → AW	PAT → PR	PAT × PV → PR	PV → PR → AW
Full model	−0.357 (<0.001)	0.279 (<0.001)	−0.286 (<0.001)	−0.391 (<0.001)	−0.162 (0.001)	−0.080 (0.001)
PR2 removed	−0.347 (<0.001)	0.282 (<0.001)	−0.303 (<0.001)	−0.368 (<0.001)	−0.169 (<0.001)	−0.085 (<0.001)
PR4 removed	−0.361 (<0.001)	0.275 (<0.001)	−0.280 (<0.001)	−0.404 (<0.001)	−0.152 (0.001)	−0.077 (0.001)
PV4 removed	−0.344 (<0.001)	0.240 (0.001)	−0.301 (<0.001)	−0.405 (<0.001)	−0.172 (<0.001)	−0.072 (0.003)
AW1 removed	−0.361 (<0.001)	0.279 (<0.001)	−0.247 (<0.001)	−0.391 (<0.001)	−0.162 (0.001)	−0.069 (0.002)
All four removed	−0.343 (<0.001)	0.247 (<0.001)	−0.276 (<0.001)	−0.385 (<0.001)	−0.164 (0.001)	−0.068 (0.003)

Note: Values are standardized path coefficients (β), with p values in parentheses. The full model retained all original indicators. The sensitivity specifications excluded PR2, PR4, PV4, and AW1 individually and simultaneously.

Table A4. Variable Codebook.

Variable	Description	Measurement/Coding
PV	Perceived Privacy Invasion	PV1–PV4; five-point Likert scale
PR	Psychological Resistance	PR1–PR4; five-point Likert scale
PAT	Perceived Algorithm Transparency	PAT1–PAT4; five-point Likert scale
AW	Consumer Adoption Willingness	AW1–AW4; five-point Likert scale
Age group	Age grouping used for MGA	18–29; 30–49; 50+
Gender	Respondent gender	Categorical
Region	Respondent location	Categorical
Monthly income	Respondent monthly income	Categorical
Education	Highest educational level	Categorical

References

1. Dwivedi, Y.K.; Hughes, L.; Ismagilova, E.; Aarts, G.; Coombs, C.; Crick, T.; Duan, Y.; Dwivedi, R.; Edwards, J.; Eirug, A.; et al. Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy. *Int. J. Inf. Manag.* **2021**, *57*, 101994. [CrossRef]
2. Necula, S.-C.; Păvăloaia, V.-D. AI-Driven Recommendations: A Systematic Review of the State of the Art in E-Commerce. *Appl. Sci.* **2023**, *13*, 5531. [CrossRef]
3. Shin, D. How Do Users Interact with Algorithm Recommender Systems? The Interaction of Users, Algorithms, and Performance. *Comput. Hum. Behav.* **2020**, *109*, 106344. [CrossRef]
4. Yin, J.; Qiu, X.; Wang, Y. The Impact of AI-Personalized Recommendations on Clicking Intentions: Evidence from Chinese E-Commerce. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 21. [CrossRef]
5. Hassan, N.; Abdelraouf, M.; El-Shihy, D. The Moderating Role of Personalized Recommendations in the Trust–Satisfaction–Loyalty Relationship: An Empirical Study of AI-Driven e-Commerce. *Future Bus. J.* **2025**, *11*, 66. [CrossRef]
6. Hu, S.; Liu, J.; Li, H.; Yin, J.; Liu, X. Exploring the Mechanism of AI-Powered Personalized Product Recommendation on Generation Z Users' Spontaneous Buying Intention on Short-Form Video Platforms: A Perceived Evaluation Perspective. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 290. [CrossRef]

7. Zhu, X.; Pongsakornrungsilp, S.; Pongsakornrungsilp, P.; Kumari, A. How Perceived Accuracy Drives Adoption of AI Personalized Recommendations: A Moderated Mediation Model. *Emerg. Sci. J.* **2026**, *10*, 1042–1067. [CrossRef]
8. Aguirre, E.; Mahr, D.; Grewal, D.; De Ruyter, K.; Wetzels, M. Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *J. Retail.* **2015**, *91*, 34–49. [CrossRef]
9. Bleier, A.; Eisenbeiss, M. The Importance of Trust for Personalized Online Advertising. *J. Retail.* **2015**, *91*, 390–409. [CrossRef]
10. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and Human Behavior in the Age of Information. *Science* **2015**, *347*, 509–514. [CrossRef] [PubMed]
11. Dinev, T.; Hart, P.; Mullen, M.R. Internet Privacy Concerns and Beliefs about Government Surveillance—An Empirical Investigation. *J. Strateg. Inf. Syst.* **2008**, *17*, 214–233. [CrossRef]
12. Cloarec, J. The Personalization–Privacy Paradox in the Attention Economy. *Technol. Forecast. Soc. Change* **2020**, *161*, 120299. [CrossRef]
13. Ameen, N.; Hosany, S.; Paul, J. The Personalisation-Privacy Paradox: Consumer Interaction with Smart Technologies and Shopping Mall Loyalty. *Comput. Hum. Behav.* **2022**, *126*, 106976. [CrossRef]
14. Canhoto, A.I.; Keegan, B.J.; Ryzhikh, M. Snakes and Ladders: Unpacking the Personalisation-Privacy Paradox in the Context of AI-Enabled Personalisation in the Physical Retail Environment. *Inf. Syst. Front.* **2024**, *26*, 1005–1024. [CrossRef] [PubMed]
15. Wang, Y.; Zhu, J.; Liu, R.; Jiang, Y. Enhancing Recommendation Acceptance: Resolving the Personalization–Privacy Paradox in Recommender Systems: A Privacy Calculus Perspective. *Int. J. Inf. Manag.* **2024**, *76*, 102755. [CrossRef]
16. Hernández, P.; Morales, A.J.; Neeman, Z.; Pavía, J.M. Exploring the Privacy Paradox: An Experimental Investigation of Privacy-Preserving Behavioral Responses in Online Shopping. *J. Behav. Exp. Econ.* **2026**, *121*, 102504. [CrossRef]
17. Shin, D. The Effects of Explainability and Causability on Perception, Trust, and Acceptance: Implications for Explainable AI. *Int. J. Hum.-Comput. Stud.* **2021**, *146*, 102551. [CrossRef]
18. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *Manag. Inf. Syst. Q.* **1989**, *13*, 319–340. [CrossRef] [PubMed]
19. Martin, K.D.; Murphy, P.E. The Role of Data Privacy in Marketing. *J. Acad. Mark. Sci.* **2017**, *45*, 135–155. [CrossRef]
20. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
21. Tucker, C.E. Social Networks, Personalized Advertising, and Privacy Controls. *J. Mark. Res.* **2014**, *51*, 546–562. [CrossRef]
22. Brehm, J.W. *A Theory of Psychological Reactance*; Academic Press: New York, NY, USA, 1966.
23. Brehm, S.S.; Brehm, J.W. *Psychological Reactance: A Theory of Freedom and Control*; Academic Press: New York, NY, USA, 1981.
24. Felzmann, H.; Villaronga, E.F.; Lutz, C.; Tamò-Larrieux, A. Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns. *Big Data Soc.* **2019**, *6*, 2053951719860542. [CrossRef]
25. Ning, X.; Lu, Y.; Li, W.; Gupta, S. How Transparency Affects Algorithmic Advice Utilization: The Mediating Roles of Trusting Beliefs. *Decis. Support Syst.* **2024**, *183*, 114273. [CrossRef]
26. Wang, Y.X. *Research on the Influencing Factors of Adoption Intention of AI Personalised Recommendation Service*; Beijing University of Posts and Telecommunications: Beijing, China, 2024.
27. Thibaut, J.W.; Kelley, H.H. *The Social Psychology of Groups*, 1st ed.; Routledge: London, UK, 2017.
28. Laufer, R.S.; Wolfe, M. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *J. Soc. Issues* **1977**, *33*, 22–42. [CrossRef]
29. Culnan, M.J. Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing. *J. Direct Mark.* **1995**, *9*, 10–19. [CrossRef]
30. Alhelaly, Y.; Dhillon, G.; Oliveira, T. The Impact of Privacy Intrusiveness on Individuals' Responses and Engagement Toward Personalization in Online Interactive Advertising. *J. Interact. Advert.* **2025**, *25*, 38–60. [CrossRef]
31. Park, K.; Yoon, H.Y. Beyond the Code: The Impact of AI Perceived Algorithm Transparency Signaling on User Trust and Relational Satisfaction. *Public Relat. Rev.* **2024**, *50*, 102507. [CrossRef]
32. Sun, Y.; Liao, M.; Sundar, S.S.; Walther, J.B. Does Transparency Matter When an AI System Meets Performance Expectations? An Experiment with an Online Dating Site. *Comput. Hum. Behav.* **2026**, *177*, 108875. [CrossRef]
33. Awad, N.F.; Krishnan, M.S. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization1. *Manag. Inf. Syst. Q.* **2006**, *30*, 13–28. [CrossRef]
34. Magano, J.; Rebelo, S. Trust-First Personalization in Fashion E-Commerce: An Association-Based Model Linking Perceived Personalization, Surveillance, Privacy-Violation, and Purchase Intention. *J. Theor. Appl. Electron. Commer. Res.* **2026**, *21*, 139. [CrossRef]
35. Nusir, O.M.; Wel, C.A.C.; Ab Hamid, S.N. When AI Conversations Become Advertising Data: Algorithmic Trust, Privacy Calculus, and Purchase Intention in GenAI-Personalized Social Commerce. *J. Theor. Appl. Electron. Commer. Res.* **2026**, *21*, 197. [CrossRef]
36. Spais, G.; Phau, I.; Jain, V. AI Marketing and AI-Based Promotions Impact on Consumer Behavior and the Avoidance of Consumer Autonomy Threat. *J. Consum. Behav.* **2024**, *23*, 1053–1056. [CrossRef]

37. Chen, T.; Liu, F.; Shen, X.-L.; Wu, J.; Liu, Y. Conceptualization of Privacy Concerns and Their Influence on Consumers' Resistance to AI-Based Recommender Systems in e-Commerce. *Ind. Manag. Data Syst.* **2025**, *125*, 1844–1868. [CrossRef]
38. Quyên, N.D.T. *The Effect of Psychological Ownership on Customer Behaviors in Music Streaming Service Context*; Digital Library of University of Economics Ho Chi Minh City: Ho Chi Minh City, Vietnam, 2024.
39. Slivkin, N.; Elgaaied-Gambier, L.; Hamdi-Kidar, L. Is Virtual Reality Lonely? The VR–Isolation Stereotype and Its Impact on VR Adoption. *Psychol. Mark.* **2025**, *42*, 1110–1131. [CrossRef]
40. Mou, Y.; Meng, X. Alexa, It Is Creeping over Me—Exploring the Impact of Privacy Concerns on Consumer Resistance to Intelligent Voice Assistants. *Asia Pac. J. Mark. Logist.* **2024**, *36*, 261–292. [CrossRef]
41. Mao, Z.; Liu, L.; Fang, Z. Influencing Factors of Native Advertising Avoidance Based on Interactive Media. In *2024 International Conference on Culture-Oriented Science & Technology (CoST)*; IEEE Computer Society: Los Alamitos, CA, USA, 2024; pp. 162–168.
42. Shin, D.; Rasul, A.; Fotiadis, A. Why Am I Seeing This? Deconstructing Algorithm Literacy through the Lens of Users. *Internet Res.* **2022**, *32*, 1214–1234. [CrossRef]
43. Oncioiu, I. AI Transparency and User Behavior in Human–AI Collaboration: Evidence from E-Commerce Recommendation Systems. *J. Theor. Appl. Electron. Commer. Res.* **2026**, *21*, 153. [CrossRef]
44. Dendrinos, K.; Spais, G. An Investigation of Selected UTAUT Constructs and Consumption Values of Gen Z and Gen X for Mobile Banking Services and Behavioral Intentions to Facilitate the Adoption of Mobile Apps. *J. Mark. Anal.* **2024**, *12*, 492–522. [CrossRef]
45. Blumberg, B.; Cooper, D.R.; Schindler, P.S. *Business Research Methods*, 4th ed.; McGraw-Hill Education: New York, NY, USA, 2014.
46. Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*, 7th ed.; Pearson: Harlow, UK, 2016.
47. China Internet Network Information Center (CNNIC). *The 55th Statistical Report on China's Internet Development*; China Internet Network Information Center (CNNIC): Beijing, China, 2024.
48. Hair, J.F., Jr.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed.; SAGE Publications: Thousand Oaks, CA, USA, 2021.
49. Kock, N.; Hadaya, P. Minimum Sample Size Estimation in PLS-SEM: The Inverse Square Root and Gamma-exponential Methods. *Inf. Syst. J.* **2018**, *28*, 227–261. [CrossRef]
50. Shi, Y.; Mao, Y.; Zhang, G. A Meta-Analysis Research on Influencing Factors of Users' Adoption Intention of Personalized Algorithm Recommendation Services. *Libr. J.* **2024**, *43*, 96–108.
51. Dillman, D.A.; Smyth, J.D.; Christian, L.M. *Internet, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 3rd ed.; Wiley: Hoboken, NJ, USA, 2009.
52. Singh, A.S.; Masuku, M.B. Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. *Int. J. Econ. Commer. Manag.* **2014**, *2*, 1–22.
53. Martin, K.D.; Zimmermann, J. Artificial Intelligence and Its Implications for Data Privacy. *Curr. Opin. Psychol.* **2024**, *58*, 101829. [CrossRef] [PubMed]
54. Ha, S.; Park, J.-S.; Jeong, S.W. Let Me Shop Alone: Consumers' Psychological Reactance toward Retail Robotics. *Technol. Forecast. Soc. Change* **2025**, *212*, 123962. [CrossRef]
55. Cadario, R.; Longoni, C.; Morewedge, C.K. Understanding, Explaining, and Utilizing Medical Artificial Intelligence. *Nat. Hum. Behav.* **2021**, *5*, 1636–1642. [CrossRef] [PubMed]
56. Li, Y.; Deng, X.; Hu, X.; Liu, J. The Effects of E-Commerce Recommendation System Transparency on Consumer Trust: Exploring Parallel Multiple Mediators and a Moderator. *J. Theor. Appl. Electron. Commer. Res.* **2024**, *19*, 2630–2649. [CrossRef]
57. Li, L.; Wang, T. The Impact of Product Uniqueness in AI Recommendation Systems on User Acceptance Willingness. In *Proceedings of the 2024 5th International Conference on Computer Science and Management Technology*; ACM: Xiamen, China, 2024; pp. 103–109.
58. Shmueli, G.; Sarstedt, M.; Hair, J.F.; Cheah, J.-H.; Ting, H.; Vaithilingam, S.; Ringle, C.M. Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *Eur. J. Mark.* **2019**, *53*, 2322–2347. [CrossRef]
59. Sharma, P.N.; Liengaard, B.D.; Hair, J.F.; Sarstedt, M.; Ringle, C.M. Predictive model assessment and selection in composite-based modeling using PLS-SEM: Extensions and guidelines for using CVPAT. *Eur. J. Mark.* **2023**, *57*, 1662–1677. [CrossRef]
60. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.-Y.; Podsakoff, N.P. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [CrossRef] [PubMed]
61. Kock, N. Common Method Bias in PLS-SEM: A Full Collinearity Assessment Approach. *Int. J. E-Collab.* **2015**, *11*, 1–10. [CrossRef]
62. Liang, H.; Saraf, N.; Hu, Q.; Xue, Y. Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management1. *Manag. Inf. Syst. Q.* **2007**, *31*, 59–87. [CrossRef]
63. Becker, J.-M.; Proksch, D.; Ringle, C.M. Revisiting Gaussian copulas to handle endogenous regressors. *J. Acad. Mark. Sci.* **2022**, *50*, 46–66. [CrossRef]
64. Liengaard, B.D.; Becker, J.-M.; Bennedsen, M.; Heiler, P.; Taylor, L.N.; Ringle, C.M. Dealing with regression models' endogeneity by means of an adjusted estimator for the Gaussian copula approach. *J. Acad. Mark. Sci.* **2025**, *53*, 279–299. [CrossRef]
65. Henseler, J.; Ringle, C.M.; Sarstedt, M. Testing measurement invariance of composites using partial least squares. *Int. Mark. Rev.* **2016**, *33*, 405–431. [CrossRef]

66. Hardcastle, K.; Vorster, L.; Brown, D.M. Understanding Customer Responses to AI-Driven Personalized Journeys: Impacts on the Customer Experience. *J. Advert.* **2025**, *54*, 176–195. [CrossRef]
67. Menard, P.; Bott, G.J. Artificial Intelligence Misuse and Concern for Information Privacy: New Construct Validation and Future Directions. *Inf. Syst. J.* **2025**, *35*, 322–367. [CrossRef]
68. An, G.K.; Ngo, T.T.A. AI-Powered Personalized Advertising and Purchase Intention in Vietnam's Digital Landscape: The Role of Trust, Relevance, and Usefulness. *J. Open Innov. Technol. Mark. Complex.* **2025**, *11*, 100580. [CrossRef]
69. Turki, H. AI-Powered Personalization in e-Commerce: Governance, Consumer Behavior, and Exploratory Insights from Big Data Analytics. *Technol. Soc.* **2025**, *83*, 103033. [CrossRef]
70. Aydin, S. Brand Trust in AI-Driven E-Commerce Personalization: The Well-Being–Privacy Trade-Off. *Sustainability* **2026**, *18*, 1073. [CrossRef]
71. Choi, J.; Kang, S.; Moon, J.; Jeon, S.; Lim, S. Algorithmic Transparency and Consumer Trade-Offs in AI-Based Financial E-Commerce Services. *J. Theor. Appl. Electron. Commer. Res.* **2026**, *21*, 86. [CrossRef]
72. Huang, Y.; Liu, L. The Impact of Algorithm Awareness on the Acceptance of Personalized Social Media Content Recommendation Based on the Technology Acceptance Model. *Acta Psychol.* **2025**, *259*, 105383. [CrossRef] [PubMed]
73. Hien, N.N.; Luu, D.X.; Ghi, T.N.; Nguyen, T.N. Determinants of AI-Integrated E-Commerce Acceptance: The Roles of Personal Innovativeness, Self-Efficacy, Compatibility, and Curiosity. *Hum. Behav. Emerg. Technol.* **2026**, *2026*, 5689688. [CrossRef]

https://doi.org/10.3390/jtaer21090310