

WHEN DATA SECURITY BUILDS TRUST BUT RESTRAINS PURCHASE DECISIONS

Hairul Hatami¹

¹Master of Management Program, Faculty of Economics and Business, Lambung Mangkurat University, Indonesia

Correspondensi author email: zuliahatami@gmail.com

Abstract

Artificial intelligence (AI)-personalized advertising relies on extensive consumer data, making data security a critical factor in shaping trust and purchasing responses. This study examines how perceived data security simultaneously influences consumer trust and purchase decision in AI-personalized advertising on Instagram. Using a quantitative explanatory survey, data were collected from 300 Generation Z Instagram users in Indonesia and analyzed with PLS-SEM using SmartPLS 4. The article focuses on the data-security pathway within the original structural model. The results show that perceived data security is positively associated with consumer trust ($\beta = 0.286$, $p < 0.001$), while consumer trust is positively associated with purchase decision ($\beta = 0.195$, $p = 0.001$). Perceived data security also has a positive indirect association with purchase decision through consumer trust ($\beta = 0.056$, $p = 0.002$). However, its direct association with purchase decision is negative and significant ($\beta = -0.090$, $p = 0.043$). These opposing pathways indicate competitive or inconsistent mediation. The findings suggest a security-trust-behavior asymmetry, showing that favorable security perceptions can strengthen trust without producing an equally positive direct behavioral response.

Keywords: AI-personalized advertising; Consumer trust; Data security; Purchase decision; Security-trust-behavior asymmetry

INTRODUCTION

Artificial intelligence (AI) has reshaped digital advertising by enabling firms to move beyond broad audience segmentation toward increasingly individualized and data-driven forms of personalization. In AI-powered personalized advertising, algorithms can process consumers' behavioral patterns, preferences, interests, and interaction histories to tailor advertising messages more closely to individual needs. This capability can improve message relevance, perceived usefulness, and the overall effectiveness of advertising in stimulating favorable consumer responses (An & Ngo, 2025). At the same time, such personalization depends heavily on the collection, processing, and use of consumer data. Consequently, the expansion of AI-driven marketing has intensified concerns surrounding data confidentiality, unauthorized use, cyber threats, and the transparency of data-handling practices (Alhitmi et al., 2024). Recent literature therefore increasingly treats personalization not simply as a technological advantage, but as a data-governance issue in which greater relevance may

coexist with heightened concerns about privacy, surveillance, and control over personal information (Yildirim & Gündüzyeli, 2026). This tension is particularly important in social media environments, where personalized advertising is embedded within continuous interaction and extensive behavioral data collection.

From a conventional consumer-behavior perspective, perceived data security should function as a protective cue that reduces uncertainty and vulnerability in technology-mediated interactions. When consumers believe that their personal information is securely managed and protected from misuse, such perceptions provide a basis for greater confidence in the system and in the actors responsible for handling their data. Research on AI-driven marketing has consistently linked security and privacy practices with consumer confidence, while human–AI research shows that system characteristics that enhance transparency, accountability, and interpretability can strengthen trust in AI-mediated decisions (Alhitmi et al., 2024; Shin, 2021). Trust is particularly important in AI-based advertising because consumers must accept a degree of vulnerability when relying on algorithmically generated recommendations or personalized messages. In the context of AI-powered personalized advertising, trust has also been identified as a significant predictor of purchase intention, indicating that consumers who regard AI-mediated recommendations as credible are more willing to act on them (An & Ngo, 2025). Evidence from Indonesian e-commerce likewise suggests that perceived security and consumer trust are significantly associated with online purchase decisions, reinforcing the conventional expectation that stronger protection and confidence should correspond with more favorable purchasing responses (Ardialis & Hayani, 2023).

However, the conventional expectation that stronger data-related assurances should translate into uniformly favorable consumer responses becomes less straightforward in personalized advertising environments. Personalization creates value precisely because algorithms can infer consumers' needs from increasingly detailed information, yet the same data intensity may also draw attention to how much a platform knows about its users. Recent evidence demonstrates that positive and negative evaluations can emerge simultaneously. Nusir et al. (2026), for example, show that GenAI-based advertising personalization increases perceived personalization value while also heightening privacy concerns; the former strengthens algorithmic trust, whereas the latter weakens it. Similarly, Sun et al. (2025) demonstrate experimentally that consumer responses to AI-generated personalized advertising are not necessarily linear. Moderate personalization produced the most favorable attitudes, whereas excessive personalization became less effective because perceived threat increased relative to perceived utility. Related evidence also shows that trust in AI can positively support purchasing responses while privacy concerns exert an opposing influence, illustrating that favorable evaluations of AI personalization may coexist with apprehension about the data practices underlying it (Alsaffarini & Awwad, 2026). These

findings challenge the assumption that improvements in the technical or functional quality of personalization will continuously enhance consumer responses.

This tension can be understood through complementary perspectives from Privacy Calculus Theory and approach–avoidance reasoning. Privacy calculus suggests that consumers evaluate the benefits obtained from personalization against the perceived risks associated with data collection, inference, and commercial use; consequently, appreciation of a personalized service does not necessarily eliminate concern about the data practices that make such personalization possible (Nusir et al., 2026). Evidence from personalized advertising similarly shows that personalization and perceived control can support trust, whereas privacy concerns and perceived intrusiveness are associated with less favorable consumer responses (Madane & Azeroual, 2025). Approach–avoidance reasoning further suggests that a single advertising environment can activate motivations to approach and withdraw at the same time. In AI-generated advertising, perceived utility can encourage approach, while perceived threat arising from intensive use of personal information can activate avoidance, with the balance between these evaluations shaping subsequent consumer attitudes (Sun et al., 2025). This behavioral restraint is also consistent with the broader digital advertising literature. (Çelik et al., 2023) identify psychological reactance as the most frequently employed theoretical perspective in research on digital ad avoidance and show that intrusiveness, privacy concerns, and skepticism repeatedly appear as mechanisms associated with avoidance. Thus, favorable evaluations of personalization or data protection need not imply an absence of caution.

The coexistence of these responses is also relevant in the Indonesian digital environment. Belinda & Nofitasari (2025) report a privacy-paradox pattern in which Indonesian consumers continue to value and engage with AI-driven personalization despite substantial concerns regarding transparency and the use of personal information. Such evidence suggests that acceptance of personalized digital services does not necessarily eliminate privacy-related apprehension. However, prior studies typically represent these favorable and unfavorable responses through different evaluative constructs. Personalization value, trust, and perceived control are generally associated with more favorable responses, whereas privacy concerns, intrusiveness, and perceived threat are treated as separate sources of resistance or caution (Alsaffarini & Awwad, 2026; Madane & Azeroual, 2025; Nusir et al., 2026; Sun et al., 2025).

This distinction is theoretically useful, but it leaves a narrower question insufficiently resolved: whether an ostensibly protective evaluation can itself be associated with divergent psychological and behavioral outcomes. Perceived data security is particularly relevant to this issue because it is normally understood as an assurance that personal information is protected from misuse and therefore should reduce vulnerability and strengthen trust. Yet recent reviews of AI-driven personalized advertising note that trust-related pathways remain insufficiently disaggregated and

that their direction and boundary conditions are not always clearly specified (Yildirim & Gündüzyeli, 2026). Consequently, the relationship between perceived data security, consumer trust, and purchasing behavior warrants closer examination not merely as a uniformly positive sequence, but as a potentially asymmetric process in which trust formation and behavioral response may not move in the same direction.

To address this issue, the present study places consumer trust at the center of the relationship between perceived data security and purchase decisions. Human–AI trust research provides the primary explanation for the positive psychological pathway: consumers are more willing to rely on AI-mediated systems when they perceive those systems and their underlying practices as transparent, accountable, understandable, and trustworthy (Shin, 2021). At the same time, Privacy Calculus Theory and approach–avoidance reasoning provide complementary lenses for interpreting why a favorable security evaluation may not necessarily translate into an equally favorable direct behavioral response. These perspectives suggest that consumers can recognize protective or utilitarian benefits while simultaneously evaluating the costs, vulnerabilities, or autonomy implications associated with data-intensive personalization (Nusir et al., 2026; Sun et al., 2025). The personalization–privacy paradox therefore serves here as a broader contextual frame rather than as the primary mechanism being tested. Importantly, this study does not directly measure perceived surveillance, reactance, intrusiveness, or threat. These concepts are used only to interpret the broader possibility that trust-building and behavioral restraint can coexist within AI-personalized advertising environments, rather than to claim an unobserved causal mechanism.

Against this background, this study examines how perceived data security shapes consumer trust and purchase decisions in AI-personalized advertising on Instagram. The empirical analysis draws on survey data from 300 Generation Z Instagram users in Indonesia who had previously seen or interacted with AI-based personalized advertisements and evaluates the relationships among perceived data security, consumer trust, and purchase decisions using PLS-SEM. The study addresses the following research question: How does perceived data security simultaneously shape consumer trust and purchase decisions in AI-personalized advertising? By distinguishing the direct behavioral pathway from the indirect pathway operating through consumer trust, this study makes three contributions. First, it moves beyond the broader personalization–privacy duality by focusing on what is conceptualized here as a security–trust–behavior asymmetry, in which a protective data-related evaluation need not correspond to uniformly favorable behavioral outcomes. Second, it disaggregates the role of trust to clarify how perceived data security may operate differently at psychological and behavioral levels. Third, it extends the discussion of AI-personalized advertising to an Indonesian social media context, providing evidence

from Generation Z users whose advertising experiences are closely embedded in data-intensive digital environments.

RESEARCH METHOD

This study employed a quantitative explanatory survey design to examine consumer responses to AI-personalized advertising on Instagram. The unit of analysis was the individual Instagram user who had previously been exposed to personalized advertising generated or supported by artificial intelligence. Data collection was conducted in 2025 through an online survey, an approach consistent with the digital context of the study and the characteristics of Instagram users as the target respondents. The present article draws on the original PLS-SEM dataset and structural model developed to examine multiple characteristics of AI-personalized advertising. Rather than re-estimating a separate reduced model, this article provides a focused examination of the data-security pathway within the original structural model, specifically the relationships among perceived data security, consumer trust, and purchase decision. The other constructs included in the original model remained part of the structural estimation but fall outside the analytical focus of the present article.

The target population consisted of Instagram users in Indonesia who had been exposed to AI-based personalized advertisements. Because the exact size of this population could not be determined from publicly available Instagram data, respondents were selected through non-probability purposive sampling. Eligibility criteria required respondents to be active Instagram users, to have previously seen or received AI-personalized advertisements on the platform, to fall within the targeted age range of active social-media users, and to complete the questionnaire according to the instructions provided. A total of 300 valid responses were included in the analysis. The respondents were aged between 17 and 30 years, representing predominantly Generation Z and younger digital consumers. Purposive sampling was considered appropriate because exposure to personalized advertising cannot be assumed to be uniform across Instagram users; therefore, prior exposure to such advertising was necessary to ensure that respondents could meaningfully evaluate the phenomena under investigation.

The study relied on primary quantitative data obtained directly from respondents through a structured online questionnaire. The questionnaire was administered using Google Forms and distributed through digital channels, including Instagram, WhatsApp, and other social-media platforms. Prior to full distribution, a limited pre-test was conducted to ensure that the statements were understandable and appropriate to the research context. All measurement items used a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*).

Although the original research instrument contained 26 indicators covering seven constructs, the present article reports measurement properties only for the three

constructs relevant to its analytical focus. Perceived data security was represented by four indicators (KD1–KD4), consumer trust by four indicators (KK1–KK4), and purchase decision by three indicators (KP1–KP3), resulting in 11 indicators discussed in this article. Perceived data security captured respondents' evaluations of the protection and responsible management of personal information in AI-personalized advertising. Consumer trust represented confidence in the reliability and integrity of the AI-mediated advertising environment, while purchase decision reflected consumers' evaluations and purchasing responses following exposure to personalized advertisements. The measurement of perceived data security was developed with reference to (Alhitmi et al., 2024), while the trust and purchase-decision measures were grounded in the theoretical and operational sources used in the original research instrument.

Data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4. The analytical process included data screening, measurement-model evaluation, structural-model assessment, and significance testing through bootstrapping. Prior to model estimation, responses were examined for completeness and consistency, and Likert-scale responses were coded numerically for statistical analysis. The measurement model was evaluated in terms of indicator reliability, convergent validity, internal consistency reliability, and discriminant validity. Indicator loadings of at least .70 were considered acceptable, while convergent validity was assessed using average variance extracted (AVE), with values above .50 indicating that a construct explained more than half of the variance in its indicators. Internal consistency reliability was evaluated using Cronbach's alpha and composite reliability (ρ_c), with values exceeding .70 considered acceptable. Discriminant validity was primarily examined using the heterotrait–monotrait ratio (HTMT), with values below .90 indicating satisfactory distinction among constructs (Hair et al., 2019).

The structural model was assessed using path coefficients, the coefficient of determination (R^2), effect size (f^2), and predictive performance. Because the present article focuses on only one pathway within the original full structural model, the reported R^2 values represent the explanatory power of the complete model rather than the explanatory contribution of perceived data security alone. Effect sizes were interpreted using conventional PLS-SEM thresholds of approximately .02, .15, and .35 for small, medium, and large effects, respectively. Predictive performance was additionally examined using PLSpredict and Q^2 predict values, where values greater than zero indicate predictive relevance for the endogenous constructs. Statistical significance of the structural relationships was evaluated through bootstrapping using standardized path coefficients, t -statistics, and p -values, with $p < .05$ and $t > 1.96$ used as the criteria for two-tailed significance testing.

Finally, the mediation analysis focused specifically on the indirect relationship between perceived data security and purchase decision through consumer trust. The

specific indirect effect, together with the corresponding direct effect of perceived data security on purchase decision, was evaluated using bootstrap estimates, *t*-statistics, and *p*-values. This distinction is central to the analytical purpose of the article because it allows the trust-mediated pathway to be evaluated separately from the direct behavioral association. Accordingly, the article does not treat the three constructs as an independently re-estimated model; rather, it isolates and interprets the relevant direct and indirect paths from the original PLS-SEM structural model.

RESULT AND DISCUSSION

Respondent Characteristics

The analysis was based on 300 valid responses from Indonesian Instagram users who had previously been exposed to AI-personalized advertising. As shown in Table 1, the largest age group was 25–27 years, representing 51.0% of the sample, followed by respondents aged 21–24 years (21.0%), 28–30 years (18.3%), and 17–20 years (9.7%). Male respondents accounted for 58.3% of the sample, while female respondents represented 41.7%.

In terms of advertising-related experience, 91.0% of respondents reported having shown interest in, clicked, or otherwise interacted with recommended advertisements on Instagram. In addition, 83.0% reported having purchased a product after seeing an advertisement on the platform. These characteristics indicate that the respondents had substantial prior exposure to Instagram advertising and were therefore able to evaluate AI-personalized advertising based on relevant experience.

Table 1. Respondent Characteristics

Characteristic	Category	Frequency	Percentage (%)
Age	17–20 years	29	9.7
	21–24 years	63	21.0
	25–27 years	153	51.0
	28–30 years	55	18.3
Gender	Male	175	58.3
	Female	125	41.7
Interaction with recommended Instagram ads	Yes	273	91.0
	No	27	9.0
Purchase after seeing an Instagram ad	Yes	249	83.0
	No	51	17.0

Source: Primary survey data, 2026.

Measurement Model Assessment

The measurement model was evaluated before interpreting the structural relationships. Because the present article focuses on perceived data security, consumer

trust, and purchase decision, Table 2 presents only the measurement properties of these three focal constructs, although they were estimated within the original full structural model.

All 11 indicators exceeded the recommended outer-loading threshold of 0.70. The perceived data security indicators ranged from 0.870 to 0.883, consumer trust from 0.733 to 0.801, and purchase decision from 0.802 to 0.832. These results indicate satisfactory indicator reliability.

Internal consistency and convergent validity were also adequate. Cronbach's alpha values ranged from 0.747 to 0.901, while composite reliability values ranged from 0.854 to 0.931. All values exceeded the recommended threshold of 0.70. The AVE values ranged from 0.594 to 0.771 and therefore exceeded the 0.50 criterion, confirming satisfactory convergent validity.

Table 2. Measurement Model Assessment

Construct	Indicator	Outer Loading	Cronbach's α	rho_A	Composite Reliability	AVE
Perceived Data Security	KD1	0.883	0.901	0.901	0.931	0.771
	KD2	0.870				
	KD3	0.883				
	KD4	0.875				
Consumer Trust	KK1	0.770	0.772	0.774	0.854	0.594
	KK2	0.777				
	KK3	0.801				
	KK4	0.733				
Purchase Decision	KP1	0.832	0.747	0.748	0.856	0.664
	KP2	0.802				
	KP3	0.810				

Source: SmartPLS 4 output, 2026.

Discriminant validity was subsequently evaluated using the heterotrait-monotrait ratio (HTMT). As presented in Table 3, the HTMT values were 0.311 between perceived data security and consumer trust, 0.090 between perceived data security and purchase decision, and 0.569 between consumer trust and purchase decision. All values were below the 0.90 threshold, indicating that the three focal constructs were empirically distinguishable.

Table 3. Discriminant Validity Based on HTMT

Construct	Perceived Data Security	Consumer Trust	Purchase Decision
Perceived Data Security	—		

Consumer Trust	0.311	—	
Purchase Decision	0.090	0.569	—

Source: SmartPLS 4 output, 2026.

Structural Model Assessment

The explanatory and predictive performance of the original structural model is summarized in Table 4. The model produced an R^2 value of 0.304 for consumer trust and 0.455 for purchase decision, with adjusted R^2 values of 0.293 and 0.444, respectively. Accordingly, the complete set of predictors in the original model explained 30.4% of the variance in consumer trust and 45.5% of the variance in purchase decision. These values represent the explanatory power of the full structural model and should not be interpreted as variance explained by perceived data security alone.

The focal effect sizes further clarify the magnitude of the relationships examined in this article. Perceived data security produced an f^2 value of 0.116 for consumer trust, indicating a small effect under conventional benchmarks. Its direct effect on purchase decision was substantially smaller, with $f^2 = 0.013$, while consumer trust produced an f^2 value of 0.048 for purchase decision. The relatively small direct effect of perceived data security on purchase decision is particularly important for interpreting the structural results proportionately.

Predictive relevance was further assessed using PLSpredict. The Q^2 predict values were positive for both endogenous constructs, reaching 0.272 for consumer trust and 0.405 for purchase decision. These positive values indicate that the original model retained predictive relevance for both outcomes.

Table 4. Structural Model Assessment

Assessment	Consumer Trust / Path	Purchase Decision / Path
R^2	0.304	0.455
Adjusted R^2	0.293	0.444
Q^2 predict	0.272	0.405
f^2 : Data Security $\rightarrow$ outcome	0.116	0.013
f^2 : Consumer Trust $\rightarrow$ Purchase Decision	—	0.048

Source: SmartPLS 4 output, 2026.

Direct and Indirect Effects

The principal structural findings concern the relationships among perceived data security, consumer trust, and purchase decision. As shown in Table 5, perceived data security was positively and significantly associated with consumer trust ($\beta = 0.286$, $t = 5.486$, $p < 0.001$). Consumer trust was subsequently positively associated with purchase decision ($\beta = 0.195$, $t = 3.473$, $p = 0.001$).

However, the direct relationship between perceived data security and purchase decision moved in the opposite direction. Perceived data security showed a negative

and statistically significant association with purchase decision ($\beta = -0.090$, $t = 2.027$, $p = 0.043$). Although statistically significant, the magnitude of this pathway was small, as also reflected by its f^2 value of 0.013.

Table 5. Direct Effects of the Focal Structural Relationships

Relationship	β	Sample Mean	SD	t	p	Result
Perceived Data Security → Consumer Trust	0.286	0.287	0.052	5.486	< 0.001	Significant
Perceived Data Security → Purchase Decision	-0.090	-0.089	0.044	2.027	0.043	Significant
Consumer Trust → Purchase Decision	0.195	0.192	0.056	3.473	0.001	Significant

Source: SmartPLS 4 bootstrapping output, 2026.

The mediation analysis provides further insight into this pattern. Perceived data security showed a positive and significant indirect association with purchase decision through consumer trust ($\beta = 0.056$, $t = 3.053$, $p = 0.002$). Thus, higher perceived data security was associated with greater consumer trust, which in turn corresponded with more favorable purchase decisions.

Table 6. Indirect Effect of Perceived Data Security on Purchase Decision

Relationship	β	Sample Mean	SD	t	p	Result
Data Security → Consumer Trust → Purchase Decision	0.056	0.055	0.018	3.053	0.002	Significant positive indirect effect

Source: SmartPLS 4 bootstrapping output, 2026.

Taken together, the direct and indirect effects reveal two statistically significant pathways operating in opposite directions. Perceived data security was positively associated with consumer trust and indirectly supported purchase decision through trust, while its direct association with purchase decision was negative. Because the significant direct and indirect effects carry opposing signs, the pattern is consistent with competitive or inconsistent mediation (Zhao et al., 2010). Importantly, the negative direct effect should be interpreted proportionately because its coefficient and effect size are small. The findings therefore do not suggest that data security is generally detrimental to purchasing; rather, they indicate that its behavioral association is not uniformly positive once the trust-mediated pathway and the other predictors in the original structural model are considered.

Discussion

The empirical findings indicate that perceived data security plays a differentiated role in AI-personalized advertising. Its positive association with consumer trust suggests that consumers who perceive stronger protection and responsible handling of personal information are also more likely to express confidence in the AI-mediated advertising

environment. Consumer trust, in turn, is positively associated with purchase decision, indicating that security perceptions can support favorable purchasing responses when they are translated into trust.

At the same time, the negative direct association between perceived data security and purchase decision demonstrates that this relationship is not entirely linear. Although statistically significant, the direct effect is relatively small compared with the positive association between data security and trust. This difference in magnitude is important because it indicates that the negative coefficient should not be interpreted as evidence that stronger data security generally discourages purchasing. Rather, the result suggests that security perceptions may have different implications depending on whether the response is evaluated at the psychological level of trust or at the behavioral level of purchase decision.

The mediation result further clarifies this distinction. Perceived data security has a positive indirect association with purchase decision through consumer trust, while its direct association with purchase decision remains negative. Because these two statistically significant pathways carry opposite signs, the empirical pattern is consistent with competitive or inconsistent mediation (Zhao et al., 2010). In practical terms, the findings indicate that the relationship between perceived data security and purchasing responses cannot be understood adequately by examining the direct effect alone. Consumer trust represents an important intervening mechanism through which perceptions of protection become positively associated with purchase decisions.

Taken together, these findings provide the empirical basis for what this study conceptualizes as a security–trust–behavior asymmetry. Perceived data security is positively associated with consumers' psychological confidence, yet this favorable evaluation does not correspond to an equally positive direct behavioral relationship. The findings therefore establish an empirical distinction between trust formation and purchasing response. The theoretical mechanisms that may explain this asymmetry—including privacy-related caution, approach–avoidance dynamics, perceived surveillance, and psychological reactance—are examined in greater depth in the following Analysis/Discussion section.

ANALYSIS/DISCUSSION

The empirical pattern identified in this study suggests that perceived data security operates differently across psychological and behavioral pathways in AI-personalized advertising. Rather than producing a uniformly favorable response, data security strengthens consumer trust while simultaneously showing a small negative direct association with purchase decision. Because the indirect pathway through trust is positive while the direct pathway is negative, the results are consistent with a competitive or inconsistent mediation pattern (Zhao et al., 2010). This distinction is

theoretically important because it indicates that the value of perceived data security depends on the pathway through which consumer responses are evaluated.

The positive relationship between perceived data security and consumer trust is consistent with the logic of Human–AI Trust. Consumers who interact with AI-mediated advertising systems face uncertainty regarding how personal information is collected, processed, stored, and used. Perceptions that data are adequately protected can reduce vulnerability and provide reassurance that the system operates in a responsible manner. (Alhitmi et al., 2024) identify data confidentiality, cybersecurity, responsible data practices, and transparency as central concerns in AI-driven marketing, emphasizing that effective data governance is essential for maintaining consumer confidence. Similarly, Shin (2021) shows that trust in AI systems is supported by qualities such as transparency, accountability, and explainability, which help users interpret otherwise opaque algorithmic processes. From this perspective, perceived data security functions as a protective signal that reduces uncertainty and supports confidence in AI-personalized advertising.

The positive relationship between consumer trust and purchase decision further reinforces the importance of trust as a psychological mechanism. Trust reduces uncertainty when consumers evaluate recommendations generated through algorithmic systems and provides a basis for acting on those recommendations. This interpretation is consistent with An & Ngo (2025), who show that trust contributes significantly to purchase intention in AI-powered personalized advertising. Nusir et al. (2026) similarly identify algorithmic trust as an important determinant of purchase intention in GenAI-personalized social commerce. Together, these findings support the argument that perceived data security can contribute to purchasing responses when its protective value is translated into consumer trust.

However, the negative direct association between perceived data security and purchase decision indicates that this trust-based process does not capture the entire behavioral meaning of security perception. The result should not be interpreted as evidence that data security discourages purchasing. The direct effect is small, and the stronger positive pathway through trust remains central to the model. Instead, the negative direct relationship suggests that favorable perceptions of protection may coexist with other forms of caution that influence behavioral responses independently of trust. This direction is particularly noteworthy when compared with conventional e-commerce evidence. Ardialis & Hayani (2023), for example, reported positive and significant relationships between security, trust, and online purchase decisions in an Indonesian marketplace context. The contrast suggests that security perceptions may take on a more complex behavioral meaning when embedded in AI-personalized advertising, where protection is closely connected with extensive data processing and individualized targeting.

Privacy Calculus Theory provides one useful framework for understanding this coexistence. Consumers in personalized advertising environments do not evaluate benefits and risks separately. Instead, they weigh the advantages of personalization against the perceived costs associated with data collection and commercial use. Stubenvoll et al. (2024) describe targeted-advertising responses through a similar cost–benefit process, showing that personalization can improve relevance and usefulness while privacy concerns simultaneously create perceived costs. Nusir et al. (2026) offer more direct evidence of this duality in AI-related advertising by demonstrating that GenAI personalization can increase both personalization value and privacy concern. Alsaffarini & Awwad (2026) similarly show that consumers may value personalized marketing while privacy concerns continue to shape perceptions of its effectiveness. Madane & Azeroual (2025) further demonstrate that perceived control contributes strongly to trust in personalized advertising, whereas intrusiveness and concerns regarding data management can weaken favorable responses even when targeting is perceived as relevant. These findings indicate that favorable and unfavorable evaluations do not necessarily cancel each other out; they may operate simultaneously within the same consumer decision process.

This coexistence is also visible within the Indonesian digital-marketing environment. Belinda & Nofitasari (2025) describe consumer responses to AI-based personalization as ambivalent: consumers appreciate the relevance generated by personalization while continuing to express concerns regarding personal-data privacy. Such evidence reinforces the importance of treating acceptance of AI personalization and concern about its data practices as potentially simultaneous rather than mutually exclusive responses. In this respect, the present findings extend an existing contextual tension by showing that divergence can also emerge within the behavioral consequences of an ostensibly protective evaluation such as perceived data security.

An approach–avoidance perspective further explains why this duality can emerge. Sun et al. (2025) demonstrate experimentally that responses to AI-generated personalized advertising are not necessarily linear because personalization can activate both perceived utility and perceived threat. Moderate personalization produced the most favorable attitudes, whereas stronger personalization became less favorable when threat increased relative to utility. Their findings illustrate that approach and avoidance motivations can operate concurrently. Applied cautiously to the present study, this perspective suggests that consumers may perceive data protection as reassuring while also becoming more conscious of the scale of information required to produce individualized advertising. Thus, a protective evaluation does not necessarily eliminate all forms of behavioral caution.

Research on psychological reactance, perceived surveillance, and advertising resistance provides additional theoretical context. Çelik et al. (2023) identify privacy concerns, intrusiveness, skepticism, and psychological reactance as recurring

explanations of digital advertising avoidance. Stubenvoll et al. (2024) likewise suggest that privacy concerns can generate avoidance when targeted advertising is perceived as intruding into private space or limiting personal freedom. Segijn et al. (2023) further show that increased awareness of personalized advertising practices can heighten perceived surveillance and contribute to resistance. More recent evidence strengthens this interpretation. Segijn et al. (2024) found that repeated synced-advertising exposure increased perceived surveillance, which could undermine favorable brand responses. Segijn & Strycharz (2025) similarly show that consumers evaluating advertising-related dataveillance place considerable importance on awareness and control, while some also express privacy cynicism arising from a perceived lack of control over the collection and use of their information. Together, these studies illustrate how awareness of data-intensive personalization can produce psychological responses that are not necessarily resolved simply because data practices are perceived as secure.

Nevertheless, these mechanisms must be interpreted cautiously in relation to the present findings. The study did not directly measure privacy concern, perceived surveillance, intrusiveness, psychological reactance, privacy cynicism, or perceived threat. It would therefore be inappropriate to claim that any of these variables caused the negative direct relationship between perceived data security and purchase decision. Rather, they provide theoretically plausible explanations that can guide future research. The present evidence establishes the existence of an asymmetrical pattern, but not the specific psychological process responsible for the negative direct pathway.

This distinction contributes to the broader personalization–privacy literature. Previous studies generally represent favorable and unfavorable responses through separate constructs. Nusir et al. (2026), for example, distinguish personalization value from privacy concern, while Sun et al. (2025) distinguish perceived utility from perceived threat. Similar separation appears in Madane & Azeroual (2025), where perceived control and trust represent favorable evaluations while intrusiveness and data-related concerns represent adverse ones. Alsaffarini & Awwad (2026) likewise position the benefits of personalized marketing alongside continuing privacy concerns. In these studies, positive and negative responses originate from conceptually distinct consumer evaluations. The present study reveals a different pattern: divergence appears around the same ostensibly protective construct—perceived data security.

This pattern is conceptualized here as a security–trust–behavior asymmetry. The concept refers to the separation between a favorable protective evaluation, its positive psychological consequence, and its non-equivalent direct behavioral outcome. It suggests that trust formation and purchasing response should not automatically be treated as parallel consequences of perceived security. Yildirim & Gündüzyeli (2026) similarly emphasize that trust occupies a central but fragile position in AI-driven advertising and that consumer responses depend on the interaction of transparency, perceived control, legitimacy of data practices, and privacy-related tensions. By

disaggregating the direct and trust-mediated pathways, the present study provides a more specific explanation of how security perceptions may operate differently across stages of consumer response.

The findings also refine the theoretical role of consumer trust. Trust is not merely another favorable attitude positioned between security perception and purchase decision. Instead, it functions as a mechanism that transforms a protective evaluation into a positive behavioral response. This is particularly evident because the indirect pathway through trust is positive despite the opposing direct relationship. In other words, security becomes behaviorally supportive when it is translated into trust. The mediation result therefore demonstrates that the meaning of perceived data security changes depending on whether it is evaluated at the psychological or behavioral level.

From a managerial perspective, the results suggest that firms should not treat data protection purely as a technical or regulatory requirement. Strong security practices remain essential because they contribute to consumer trust, but their effectiveness also depends on how consumers experience and interpret those practices. Advertisers and platforms should therefore combine credible data protection with understandable explanations, meaningful user control, and personalization practices that preserve consumer agency. This implication is reinforced by Madane & Azeroual (2025), who highlight the importance of perceived control in trust formation, and Segijn & Strycharz (2025), whose findings indicate that consumers value awareness and control over advertising-related dataveillance. The objective is therefore not to reduce security communication, but to communicate protection in ways that reassure consumers without allowing extensive monitoring or data extraction to dominate the advertising experience.

Overall, the study shows that perceived data security should not be understood as a simple linear antecedent of favorable purchasing responses. Its strongest contribution appears through trust formation, while the remaining negative direct association indicates that security-related evaluations may also involve behavioral considerations that are not captured by trust alone. Future research should therefore incorporate privacy concern, perceived surveillance, intrusiveness, psychological reactance, privacy cynicism, perceived control, and perceived threat into more comprehensive models. Experimental and longitudinal designs would also help determine whether the observed asymmetry changes across different forms of personalization, security disclosure, and repeated exposure to AI-personalized advertising.

CONCLUSION

This study shows that perceived data security does not generate a uniformly positive behavioral response in AI-personalized advertising. Perceived data security was positively associated with consumer trust, and consumer trust was positively associated

with purchase decision. The indirect relationship between perceived data security and purchase decision through consumer trust was also positive and significant. However, perceived data security simultaneously showed a small negative direct association with purchase decision. The opposing signs of the direct and indirect pathways indicate a competitive or inconsistent mediation pattern.

These findings demonstrate that the psychological and behavioral consequences of perceived data security should not automatically be treated as equivalent. Data security can strengthen confidence in AI-mediated advertising through trust while still showing a different direct relationship with purchasing responses. This pattern is conceptualized as a security–trust–behavior asymmetry, highlighting the importance of distinguishing trust formation from subsequent behavioral outcomes in AI-personalized advertising.

Practically, advertisers and digital platforms should continue to strengthen data protection while integrating security with transparent data practices, understandable communication, and meaningful consumer control. The findings should nevertheless be interpreted within the study's cross-sectional design and the absence of direct measures of privacy concern, perceived surveillance, intrusiveness, or psychological reactance. Future research should examine these mechanisms using experimental or longitudinal designs to clarify why favorable security perceptions may coexist with restrained behavioral responses.

REFERENCE

- Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: An exploration into possible solutions. *Cogent Business & Management*, 11(1), 2393743. <https://doi.org/10.1080/23311975.2024.2393743>
- Alsaffarini, E., & Awwad, B. S. (2026). The Impact of Data Privacy Concerns on Customized Marketing Effectiveness: Evidence from the Jordanian Market. *EuroMid Journal of Business and Tech-Innovation (EJBTI)*, 5(2), 20–32. <https://doi.org/10.51325/dt3jr955>
- An, G. K., & Ngo, T. T. A. (2025). AI-powered personalized advertising and purchase intention in Vietnam's digital landscape: The role of trust, relevance, and usefulness. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(3), 100580. <https://doi.org/10.1016/j.joitmc.2025.100580>
- Ardialis, M. B., & Hayani, N. (2023). Pengaruh Kepercayaan, Keamanan, dan Persepsi Resiko terhadap Keputusan Pembelian Online pada Marketplace Lazada. *Indonesian Journal of Business Economics and Management*, 2(1), 1–8. <https://doi.org/10.57152/ijbem.v2i1.470>

- Belinda, B., & Nofitasari, D. (2025). Peran Artificial Intelligence dalam Digital Marketing dan Dampaknya terhadap Perilaku Konsumen Tahun 2025. *Jurnal GICI Jurnal Keuangan Dan Bisnis*, 17(1), 100–108. <https://doi.org/10.58890/jkb.v17i1.391>
- Çelik, F., Çam, M. S., & Koseoglu, M. A. (2023). Ad avoidance in the digital context: A systematic literature review and research agenda. *International Journal of Consumer Studies*, 47(6), 2071–2105. <https://doi.org/10.1111/ijcs.12882>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Madane, Y., & Azeroual, M. (2025). Perceived Intrusiveness vs. Relevance: A PLS-SEM Analysis of Personalized Advertising in Morocco. *Digital*, 5(4), 63. <https://doi.org/10.3390/digital5040063>
- Nusir, O. M., Che Wel, C. A., & Ab Hamid, S. N. (2026). When AI conversations become advertising data: Algorithmic trust, privacy calculus, and purchase intention in GenAI-personalized social commerce. *Journal of Theoretical and Applied Electronic Commerce Research*, 21, 197. <https://doi.org/10.3390/jtaer21070197>
- Segijn, C. M., Kim, E., Sifaoui, A., & Boerman, S. C. (2023). When you realize that big brother is watching: How informing consumers affects synced advertising effectiveness. *Journal of Marketing Communications*, 29(4), 317–338. <https://doi.org/10.1080/13527266.2021.2020149>
- Segijn, C. M., Kim, E., & van Ooijen, I. (2024). The Role of Perceived Surveillance and Privacy Cynicism in Effects of Multiple Synced Advertising Exposures on Brand Attitude. *Journal of Current Issues and Research in Advertising*, 45(4), 506–522. <https://doi.org/10.1080/10641734.2024.2318711>
- Segijn, C. M., & Strycharz, J. (2025). Transparency, Awareness, and Privacy Cynicism: Exploring Appropriate Dataveillance for Personalized Advertising Through Qualitative Interviews. *Journal of Interactive Advertising*, 25(3), 272–284. <https://doi.org/10.1080/15252019.2025.2546338>
- Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies*, 146, 102551. <https://doi.org/10.1016/j.ijhcs.2020.102551>
- Stubenvoll, M., Binder, A., Noetzel, S., Hirsch, M., & Matthes, J. (2024). Living is easy with eyes closed: Avoidance of targeted political advertising in response to privacy concerns, perceived personalization, and overload. *Communication Research*, 51(2), 203–227. <https://doi.org/10.1177/00936502221130840>
- Sun, H., Xie, P., & Sun, Y. (2025). The inverted U-shaped effect of personalization on consumer attitudes in AI-generated ads: Striking the right balance between utility and threat. *Journal of Advertising Research*, 65(2), 237–258. <https://doi.org/10.1080/00218499.2025.2462405>

- Yildirim, N., & Gündüzyeli, B. (2026). The personalization–privacy paradox in AI-driven programmatic advertising: Implications for digital marketing sustainability. *Journal of Theoretical and Applied Electronic Commerce Research*, 21, 179. <https://doi.org/10.3390/jtaer21060179>
- Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, 37(2), 197–206. <https://doi.org/10.1086/651257>