EuroMid Journal of Business and Tech-Innovation (EJBTI)
https://iejbti.com

Online ISSN: 3062-2131
Print ISSN: xxxx-xxxx

The Impact of Data Privacy Concerns on Customized Marketing Effectiveness: Evidence from the Jordanian Market

Enas Alsaffarini
College of Economics and Business, Palestine Technical University, Kadoorie, Palestine
E-mail: e.thabit@ptuk.edu.ps

Bahaa Subhi Awwad *
College of Business and Finance, Ahlia University, Manama, Bahrain
E-mail: r.awwadb@hotmail.com
*Corresponding Author

Received: December 2025; **Accepted**: May 2026

Abstract: Within the context of Privacy Calculus Theory, this study investigates the relationship between consumers' data privacy concerns and the perceived effectiveness of personalized marketing. Using a quantitative survey, the study examines how consumers weigh the benefits of personalization against the risks to their privacy in the context of digital marketing. The findings show that while consumers value personalized marketing, privacy concerns influence their overall perception of its effectiveness. High privacy concerns are linked to lower perceptions of personalized marketing strategies, underscoring the conflict between utility and risk. The study applies Privacy Calculus Theory to marketing effectiveness, extending beyond disclosure intentions alone. Jordan, as a developing market, is increasingly adopting digital marketing and growing more aware of data privacy issues. The findings highlight the importance of trust-building mechanisms, privacy-sensitive personalization strategies, and organizational transparency. Companies must balance their personalization efforts with responsible data practices in order to improve customer acceptance and sustain long-term engagement.

Keywords: Digital Marketing, Data Privacy Concerns (DPC), Consumer Trust, Personalization-Privacy Paradox, Personalized Advertising.

Type: Research Paper

DOI: 10.51325/dt3jr955

1. Introduction

The field of digital marketing faces an inherent conflict between hyper-personalized messaging—enabled by advanced data analytics—and rising consumer privacy concerns stemming from data breaches and opaque data practices (Sipos, 2024). Personalized advertising, by targeting consumer behavior, holds the potential to deliver relevant messages, increase conversion rates, and foster greater customer loyalty (Tomar and Pandey, 2024; Abdel Monem, 2021; Shanahan et al., 2019; Chen et al., 2023). However, growing societal awareness of surveillance capitalism and algorithmic manipulation increasingly overshadows these benefits (Eg et al., 2023; Darmody and Zwick, 2020; Stahl et al., 2023).

This “privacy-personalization paradox” makes it difficult for marketers to balance data-driven commercial practice with evolving consumer expectations of digital rights and responsible data stewardship (Saura, 2024; Kawaf et al., 2024). Understanding the nature, direction, and magnitude of the relationship between Data Privacy Concerns (DPC) and Perceived Effectiveness of Personalized Marketing (PEPM) is essential for developing future-proof, regulation-compliant, and consumer-centric marketing strategies, particularly in an era of strict global regulations such as GDPR and CCPA (Pizzey et al., 2025; Yadav et al., 2024; Lina and Setiyanto, 2021; Teraiya and Krishnamurthy, 2025). This research uses rigorous quantitative analysis to determine how high DPC levels affect PEPM, and offers practical recommendations for practitioners navigating this evolving landscape. As Jordanian consumers increasingly embrace digital marketing and become more aware of their data privacy rights, striking this balance has become increasingly important.

This study contributes three theoretical and empirical perspectives to the personalized marketing and privacy literature. First, it applies Privacy Calculus Theory to customized marketing effectiveness by assessing whether consumers’ DPC limit the perceived efficacy of personalized marketing—not merely their disclosure intention or willingness to share data. Second, the study provides context from Jordan, an emerging market with rising digital marketing adoption and developing consumer privacy awareness and regulatory consciousness. Prior research has largely focused on Western or highly regulated digital ecosystems, overlooking this context. Third, the study demonstrates that privacy concerns matter not only for compliance and ethics, but also for marketing effectiveness, as they are linked to lower perceived efficacy of personalized marketing. In doing so, the study extends Privacy Calculus Theory and evaluates its applicability in an emerging-market setting.

2. Theoretical Context and Hypothesis Development

Grounded in Privacy Calculus Theory (PCT), this research conceptualizes privacy decisions as rational cost-benefit trade-offs, assuming that consumers continuously weigh the cognitive value of personalization against salient privacy risks (Mini, 2017; Fu et al., 2023; Dienlin, 2023; Zhu et al., 2017; Teraiya and Krishnamurthy, 2025; Fernandes and Pereira, 2021; Plangger and Montecchi, 2020). Consistent with PCT’s core assumptions, personalized content represents the primary value source—offering greater relevance, convenience, and subjective utility (Majumdar and Bose, 2016; Beke et al., 2022; Chen and Chen, 2025).

Against these benefits, consumers perceive salient threats including data collection intensity, potential for misuse, unauthorized third-party disclosure, and surveillance, all of which give rise to psychological reactance (Brinson et al., 2024; Vecchietti et al., 2025). When privacy concerns exceed this psychological threshold, consumers employ empirically validated defensive responses such as information suppression, ad blocking, cookie rejection, and deliberate data distortion (Schöni et al., 2024; Parra-Arnau et al., 2014).

The theoretical model further predicts that trust acts as a mediator, with perceived integrity violations diminishing perceived marketing effectiveness regardless of contextual relevance (Isaeva et al., 2020; Solberg et al., 2022; Swani et al., 2021; Irgui and Qmichchou, 2023). Within this theoretical framework, the following hypothesis is proposed:

H1: Data Privacy Concerns (DPC) have a negative effect on the Perceived Effectiveness of Personalized Marketing (PEPM).

Figure 1 depicts the conceptual model of this study, highlighting its theoretical logic and the hypothesized relationship between the main variables. Grounded in Privacy Calculus Theory, the model posits that DPC reduce personalized marketing effectiveness.

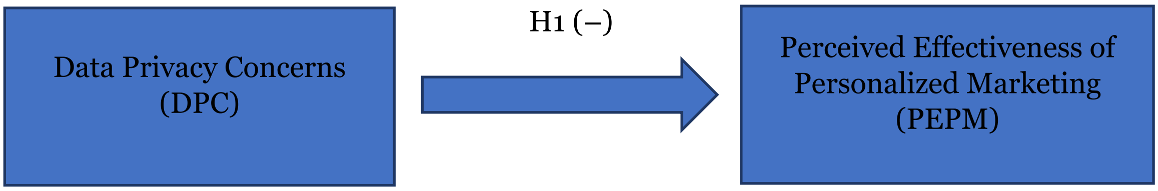

Figure 1: Conceptual Model- Privacy Calculus Theory (PCT)

As shown in Figure 1, DPC are hypothesized to negatively affect PEPM. According to Privacy Calculus Theory, consumers are less likely to view personalized marketing activities favorably when they perceive heightened privacy concerns, even if such marketing is relevant or convenient.

3. Methodology

3.1. Research Design

This study employs a cross-sectional quantitative design. Primary data were collected from 235 Jordanian internet users using purposive sampling, targeting active digital consumers who are regularly exposed to personalized marketing. This approach is appropriate when respondents with specific knowledge of the topic—such as targeted advertising and data privacy—are required. Participants were recruited through online channels including Facebook, LinkedIn, email invitations, and consumer groups, all selected to reach digitally active individuals likely to engage with personalized marketing content. The sample was restricted to Jordanian internet users to ensure contextual relevance and to capture consumer attitudes in an expanding digital market.

Table 1: Demographic Characteristics of the Respondents (N = 235).

Variable	**Category**	**Frequency (N)**	**Percentage (%)**
Gender	Male	120	51.1
	Female	110	46.8
	Prefer not to say	5	2.1
Age	Under 18	10	4.3

	18–24	60	25.5
	25–34	80	34.0
	35–44	50	21.3
	45–54	25	10.6
	55 or older	10	4.3
Level of Education	High School or Lower	25	10.6
	Diploma	35	14.9
	Bachelor's	120	51.1
	Master's	45	19.1
	Doctorate or higher	10	4.3
Occupation	Student	55	23.4
	Employee	120	51.1
	Self-employed	30	12.8
	People Without Jobs	20	8.5
	Other	10	4.3
Monthly Internet Usage	Less than 10 hours	15	6.4
	10–20 hours	35	14.9
	21–40 hours	85	36.2
	More than 40 hours	100	42.6
Awareness of Data Privacy Tools	Very Low	20	8.5
	Low	35	14.9
	Moderate	80	34.0
	High	70	29.8
	Very High	30	12.8

3.2. Measurement Instruments

Two theoretically grounded measurement scales were used in this study. A multidimensional 8-item scale, derived from prior privacy research, assessed DPC related to commercial data activities (Buchanan et al., 2007; Groß, 2023). The scale measures perceived surveillance, unlawful secondary use of personal information, and loss of control over organizational data handling. Respondents were asked about continuous online monitoring, concerns about firms sharing personal data without consent, and limited control over how marketers use their information. Sample items include "Personalized advertising intrudes into my private life" and "I am concerned that companies retain my sensitive data."

A 7-item Likert scale assessed the cognitive and behavioral dimensions of marketing effectiveness, capturing PEPM. The scale covers relevance, persuasiveness, and relational outcomes. Items examined how personalized advertisements align with consumer interests, influence purchasing decisions, and shape brand perceptions. Sample items include "Personalized ads make me more likely to purchase" and "Relevant recommendations make me a more efficient shopper."

A 5-point Likert scale was used for DPC and a 7-point scale for PEPM. This difference reflects variations in construct sensitivity and measurement conventions in the prior literature. Privacy concern items benefit from a more conservative scale, while perceived efficacy constructs benefit from greater response variability. Both constructs were treated as continuous variables in the statistical analysis. Prior regression analyses have demonstrated that Likert-type scales with differing response formats are comparable, and the difference in scale format does not affect the validity or comparability of the results.

3.3. Analytical Procedures

Descriptive statistics were used to construct a complete sample profile. Respondent demographics were summarized to characterize the research population. Measures of central tendency (means) and dispersion (standard deviations) were computed at both item and construct levels to evaluate response distribution and variability. Responses were further categorized into low, medium, and high agreement or concern using established cut-off values, to facilitate interpretation.

The reliability and validity of the measurement scales were evaluated through standard statistical procedures. Cronbach's alpha was used to assess internal consistency, with values interpreted against universally accepted benchmarks. Inter-item correlation analysis was also conducted to examine the consistency of scale item responses. Scale purification was considered where necessary to enhance measurement quality and robustness.

Inferential statistics were used to examine relationships among study variables. Prior to hypothesis testing, statistical assumptions—including normality, homoscedasticity, and linearity—were verified to ensure analytical accuracy. Bivariate correlation analysis was conducted to assess initial variable associations, followed by linear regression analysis to determine the effect of DPC on PEPM.

In the regression model, PEPM was specified as the dependent variable and DPC as the independent variable. Model evaluation included analysis of coefficient estimates, standard errors, confidence intervals, and fit indices (R, R^2, and adjusted R^2). Statistical significance was assessed using F-statistics and t-values. Diagnostic procedures tested for multicollinearity using Variance Inflation Factor (VIF) and tolerance levels. Effect magnitude was interpreted using established statistical conventions to assess the practical significance of the findings. All analyses were conducted using SPSS v.28 (IBM Corporation, 2021).

4. Results

The findings provide valuable information regarding how Jordanian consumers balance their privacy concerns with their perceptions of personalized marketing strategies.

4.1. Reliability Analysis

Psychometric analysis confirmed satisfactory measurement properties for both constructs. The DPC scale demonstrated high internal consistency (Cronbach's $\alpha = 0.787$), indicating that all eight items collectively captured the latent dimensions of privacy concern—including unauthorized access, surveillance beliefs, and policy distrust. The PEPM scale was highly reliable ($\alpha = 0.882$), with its seven items assessing relevance, behavioral impact, and trust outcomes with strong inter-item consistency. Both values exceeded the minimum threshold of 0.70 (Nunnally, 1978), providing empirical support for the use of these scales in subsequent analyses.

4.2. Descriptive Statistics

Table 2: Descriptive Statistics for DPC Items (N = 235).

Item No.	Item	Mean	Std. Deviation	Agreement Degree
5	I believe that personalized advertising compromises my personal privacy.	3.87	1.28	High
4	I feel uneasy when someone accesses my online activity without my consent.	3.71	1.30	High
3	I'm hesitant to provide advertising my personal information.	3.51	1.45	Medium
7	I often avoid using internet services that request a lot of personal information.	3.47	1.46	Medium
2	I don't think I have much influence over how marketing campaigns use my personal information.	3.33	1.43	Medium
6	Companies do not do enough to protect my personal data from unauthorized access.	3.15	1.46	Medium
8	I am skeptical about the accuracy of privacy policies presented by online companies.	2.93	1.46	Medium
1	I am concerned about how companies collect and store my personal data online.	2.77	1.38	Medium
—	Total Mean – DPC	3.34	0.89	Medium

Composite measures revealed that respondents expressed a moderate level of data privacy concern (M = 3.34, SD = 0.89). Closer examination of the individual items clarifies the nature of these concerns. Item 5 received the highest mean score, indicating that respondents were most concerned about direct and visible uses of their data. In contrast, concerns about corporate data storage received the lowest ratings, suggesting that consumers may be less aware of back-end data management risks. Responses to privacy policy items reflect moderate institutional trust, indicating that consumers neither fully trust nor fully reject organizational data practices. These patterns illustrate how consumers perceive different dimensions of privacy risk.

Table 3: Descriptive Statistics for PEPM Items (N = 235).

Item No.	Item	Mean	Std. Deviation	Agreement Degree
1	Personalized advertisements increase my likelihood of making a purchase.	3.69	1.03	High
3	I often see advertisements that are personalized to my preferences and actions.	3.57	1.15	Medium
5	I am more devoted to companies who provide pertinent and personalized recommendations.	3.48	1.05	Medium
6	I'm introduced to new products that meet my demands through personalized marketing.	3.42	1.01	Medium
2	Personalized advertisements appear more beneficial and significant than generic ones.	3.38	1.17	Medium
4	Personalized marketing enhances my perception of a brand.	3.34	1.16	Medium

7	Brands that better understand my preferences through personalized marketing have my trust.	2.84	1.14	Medium
—	Total Mean – PEPM	3.39	0.84	Medium

The perceived effectiveness of personalized marketing was moderate overall (M = 3.39, SD = 0.84), with notable variation across items. Transactional outcomes, such as purchase likelihood, received higher scores, suggesting that consumers recognize the value of personalized advertising. Trust-related items scored lower, indicating that personalization is less effective at building trust and fostering long-term relationships. This reveals a disconnect between the perceived transactional value of personalized marketing and consumer trust. When considered alongside the moderate DPC scores, the findings suggest a state of cognitive tension in which consumers engage with personalized content while remaining skeptical of underlying data practices.

4.3. Hypothesis Testing: Regression Analysis

Table 4: Linear Regression Analysis Predicting PEPM (N = 235).

Unstandardized Coefficients			**Standardized Coefficients**		
Predictors	B	Std. Error	Beta	t	P value
DPC	-0.582	0.049	-0.612	-11.810	0.000
R	R Square	F	P value	Dependent Variable: PEPM	
0.612	0.374	139.472	0.000		

The regression model was statistically significant, confirming that DPC are a meaningful predictor of PEPM. The results indicate a strong negative relationship between the two variables, implying that higher privacy concerns are associated with lower perceptions of personalized marketing effectiveness. This suggests that as consumers become more concerned about data collection and usage, they evaluate personalized marketing practices more critically.

The statistically and practically significant effect confirms that privacy concerns strongly influence consumer responses to personalized marketing. Further diagnostics revealed no violations of multicollinearity or other regression assumptions, confirming the robustness of the model. These results support Hypothesis 1, demonstrating that privacy concerns reduce the perceived effectiveness of personalized marketing.

5. Discussion

These findings carry significant implications for Jordanian marketers operating in a rapidly evolving digital landscape where public awareness of data privacy is increasing.

5.1. Interpretation of Key Findings

The results offer important insights into how consumers weigh the costs and benefits of personalization in digital marketing. First, the findings confirm the privacy–personalization paradox. The moderate levels of both DPC ($M = 3.34$) and PEPM ($M = 3.39$) suggest that consumers value personalization but are uncomfortable with data collection practices. This is consistent with prior research (Kawaf et al., 2024; Dienlin, 2023) demonstrating that consumers routinely weigh privacy risks against personalization benefits. Second, the significant negative correlation between DPC and marketing effectiveness ($\beta = -0.612$, $p < .001$) indicates that privacy concerns substantially influence consumer evaluations. This supports earlier findings (Lina and Setiyanto, 2021; Yadav et al., 2024) that higher privacy concerns reduce consumer trust and engagement with personalized marketing. Notably, the magnitude of this effect suggests that privacy concerns may outweigh perceived benefits more strongly in an emerging market context than previously reported.

Third, the findings reveal a trust gap in personalized marketing. While personalized advertisements influence purchase behavior, they do not appear to build trust. Prior research (Swani et al., 2021; Isaeva et al., 2020) has established trust as a mediator of consumer responses to marketing practices. The lower trust-related scores suggest that current personalization strategies may be perceived as intrusive rather than relationship-enhancing. Overall, the findings affirm the relevance of Privacy Calculus Theory and extend it by demonstrating that privacy concerns can outweigh the perceived usefulness of personalization. This supports a risk-dominant view of consumer behavior in the context of personalized marketing.

5.2. Theoretical Contributions

This study makes two key contributions to the literature. First, whereas prior research has primarily focused on disclosure intentions, privacy risk perceptions, or willingness to share personal data, this study applies Privacy Calculus Theory directly to PEPM, demonstrating that privacy concerns can directly affect consumer perceptions of personalized marketing effectiveness. Second, by providing evidence from Jordan—an emerging market—the study broadens the geographic scope of Privacy Calculus Theory beyond Western and highly regulated digital environments. The findings confirm that the theory is relevant in developing digital contexts and that privacy concerns can meaningfully influence marketing evaluations outside Western settings. Taken together, the study empirically validates Privacy Calculus Theory in a new context and establishes a direct link between privacy concerns and marketing effectiveness.

5.3. Managerial Implications

The empirical findings carry clear managerial implications. Given that DPC negatively impact perceived marketing effectiveness ($\beta = -0.612$), firms must redesign their personalization strategies to mitigate privacy risks while maintaining relevance and value.

Bridging Transparency Deficit

Given the significant negative impact of privacy concerns on marketing effectiveness, organizations must improve data-use transparency. This involves establishing clear disclosure systems that explicitly link data collection to the value delivered to consumers. Practices that reduce uncertainty and perceived risk—such as plain-language privacy notices and real-time data-use dashboards—can help mitigate the negative effects of privacy concerns identified in this study.

Addressing Control Limitations

The privacy–personalization paradox implies that consumers are more accepting of personalization when they perceive control over their data. Firms should therefore develop granular preference management systems that allow users to control the scope of data collection and use. Enhancing perceived control reduces privacy concerns and promotes greater acceptance of personalized marketing.

Bridging Trust Gaps

The findings show that personalization influences purchasing behavior but does not build trust. To address this, firms should employ third-party certifications, transparent data policies, and visible compliance signals. Building trust is essential to ensure that personalization drives not only short-term conversions but also long-term customer relationships.

Reducing Technological Risks

Given that privacy concerns were found to significantly reduce perceived marketing effectiveness, firms should transition toward privacy-preserving technologies such as federated learning and differential privacy. These approaches enable personalization without compromising user data, thereby reducing perceived risks and improving consumer acceptance.

Enabling Privacy-Sensitive Segmentation

The variability in consumer privacy concerns points to the value of privacy-sensitive segmentation strategies. Firms can offer high-concern users low-tracking interfaces or opt-in personalization models. This study's findings suggest that accounting for privacy concern levels in segmentation can improve perceived marketing effectiveness among privacy-sensitive consumers.

6. Limitations and Future Research

6.1. Limitations

The findings should be interpreted in light of several limitations. The cross-sectional research design makes it difficult to establish causal relationships between DPC and personalized marketing effectiveness. Reverse causality is also possible, as negative experiences with personalized advertising may themselves heighten privacy concerns.

In addition, the use of non-probability sampling may reduce the generalizability of the results. The sample was dominated by active internet users with higher levels of education and employment, which may not accurately represent less digitally engaged populations, such as rural residents or those with limited technological familiarity.

Recall bias and social desirability may also have led respondents to underreport privacy concerns when evaluating personalized marketing effectiveness. Finally, the study does not account for cultural factors, regulatory awareness, or brand reputation, all of which may influence consumers' perceptions of and responses to personalized marketing.

6.2. Future Research Directions

This study opens several avenues for future research. Longitudinal designs could better establish causal relationships and track how consumer perceptions of privacy and personalization evolve in response to events such as data breaches. Cross-cultural studies are also needed to assess the generalizability of these findings and to examine how cultural dimensions such as individualism and collectivism affect the privacy–personalization trade-off, and by extension the broader applicability of Privacy Calculus Theory.

Future research could also examine how privacy-preserving technologies affect consumer perceptions of personalized marketing. A comparative study exploring how federated learning, differential privacy, and traditional data tracking differ in their effects on consumer attitudes and behavior would be particularly valuable. Combining survey-based measures with behavioral data such as click-through rates or purchase conversions could also strengthen understanding of how privacy concerns translate into actual consumer behavior.

Finally, future research should investigate the role of regulatory awareness. Examining the mediating or moderating effects of data protection regulations such as GDPR or CCPA would illuminate how policy environments shape the relationship between privacy concerns and marketing effectiveness.

7. Conclusion

This study demonstrates that higher DPC significantly limit PEPM ($\beta = -0.612$, $R^2 = 0.374$), revealing consumer ambivalence in which privacy concerns dominate perceived usefulness ($B = -0.582$). Both DPC ($M = 3.34$) and PEPM ($M = 3.39$) operate at moderate levels, confirming the coexistence of personalization value and privacy apprehension. To resolve this paradox, companies should: (1) adopt federated learning for device-level analysis and differential privacy for anonymized data processing; (2) implement real-time value exchange dashboards to achieve radical transparency; (3) apply privacy-sensitive segmentation for high-DPC consumers; and (4) align practices with international regulations such as GDPR and CCPA, treating privacy as a strategic pillar rather than a compliance obligation. Trust remains the currency of scalable personalization in the digital economy. This study advances understanding of the privacy–personalization challenge in Jordan and contributes to a growing foundation for future digital marketing research in emerging markets.

References

Abdel Monem, H. (2021). The effectiveness of advertising personalization. Journal of Design Sciences and Applied Arts, 2, 114-121. https://doi.org/10.21608/jdsaa.2021.31121.1061

Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2022). Consumers' privacy calculus: The PRICAL index development and validation. International Journal of Research in Marketing, 39, 20-41. https://doi.org/10.1016/j.ijresmar.2021.05.005

Brinson, N., Amini, B., Lemon, L., & Bawole, C. (2024). Electronic performance monitoring: The role of reactance, trust, and privacy concerns in predicting job satisfaction in the post-pandemic workplace. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18. https://doi.org/10.5817/CP2024-5-10

Buchanan, T., Joinson, A., Paine Schofield, C., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58, 157-165. https://doi.org/10.1002/asi.20459

Chen, M., & Chen, M. (2025). Privacy relevance and disclosure intention in mobile apps: The mediating and moderating roles of privacy calculus and temporal distance. Behavioral Sciences, 15, 324. https://doi.org/10.3390/bs15030324

Chen, S., Wu, Y., Deng, F., & Zhi, K. (2023). How does ad relevance affect consumers' attitudes toward personalized advertisements and social media platforms? Journal of Retailing and Consumer Services, 73, 103336. https://doi.org/10.1016/j.jretconser.2023.103336

Darmody, A., & Zwick, D. (2020). Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. Big Data & Society, 7. https://doi.org/10.1177/2053951720904112

Dienlin, T. (2023). Privacy calculus: Theory, studies, and new perspectives. In The Routledge Handbook of Privacy and Social Media (pp. 1-15). Routledge. https://doi.org/10.4324/9781003244677-8

Eg, R., Demirkol Tønnesen, Ö., & Tennfjord, M. K. (2023). A scoping review of personalized user experiences on social media. Computers in Human Behavior Reports, 9, 100253. https://doi.org/10.1016/j.chbr.2022.100253

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

Fu, J., Zhang, J., & Li, X. (2023). How do risks and benefits affect user privacy decisions? Frontiers in Psychology, 14, 1052782. https://doi.org/10.3389/fpsyg.2023.1052782

Groß, T. (2023). Toward valid and reliable privacy concern scales: The example of IUIPC-8. In N. Gerber, A. Stöver, & K. Marky (Eds.), Human Factors in Privacy Research (pp. 65-88). Springer. https://doi.org/10.1007/978-3-031-28643-8_4

IBM Corporation. (2021). IBM SPSS Statistics for Windows, Version 28.0. IBM Corp.

Irgui, A., & Qmichchou, M. (2023). Contextual marketing and information privacy concerns in m-commerce and their impact on consumer loyalty. Arab Gulf Journal of Scientific Research. https://doi.org/10.1108/AGJSR-09-2022-0198

Isaeva, N., Gruenewald, K., & Saunders, M. (2020). Trust theory and customer services research: Theoretical review and synthesis. Service Industries Journal, 40, 1-33. https://doi.org/10.1080/02642069.2020.1779225

Kawaf, F., Montgomery, A., & Thuemmler, M. (2024). Unpacking the privacy-personalisation paradox in GDPR-regulated environments. Information Technology & People, 37, 1674-1695. https://doi.org/10.1108/ITP-04-2022-0275

Lina, L. F., & Setiyanto, A. (2021). Privacy concerns in personalized advertising effectiveness on social media. Sriwijaya International Journal of Dynamic Economics and Business, 147-156. https://doi.org/10.29259/sijdeb.v1i2.147-156

Majumdar, A., & Bose, I. (2016). Privacy calculus theory and its applicability for emerging technologies. In E-Life: Web-Enabled Convergence of Commerce, Work, and Social Life (pp. 191-195). Springer. https://doi.org/10.1007/978-3-319-45408-5_20

Mini, T. (2017). Privacy calculus [Seminar thesis, University of Passau]. ResearchGate. https://www.researchgate.net/publication/322900839_Privacy_Calculus

Nunnally, J. C. (1978). Psychometric Theory (2nd ed.). McGraw-Hill.

Parra-Arnau, J., Rebollo-Monedero, D., & Forné, J. (2014). Optimal forgery and suppression of ratings for privacy enhancement in recommendation systems. Entropy, 16, 1586-1631. https://doi.org/10.3390/e16031586

Pizzey, A., Carabine, G., John, A., & Beverley, B. (2025). Consumer behavior towards personalized marketing amidst privacy concerns [Preprint]. ResearchGate. https://www.researchgate.net/publication/388491708

Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. Journal of Interactive Marketing, 50, 32-44. https://doi.org/10.1016/j.intmar.2019.10.004

Saura, J. R. (2024). Algorithms in Digital Marketing: Does Smart Personalization Promote a Privacy Paradox? SAGE. https://doi.org/10.1177/23197145241276898

Schöni, L., Kubicek, K., & Zimmermann, V. (2024). Block cookies, not websites: Analysing mental models and usability of privacy tools. Proceedings on Privacy Enhancing Technologies, 2024, 192-216. https://doi.org/10.56553/popets-2024-0012

Shanahan, T., Tran, T. P., & Taylor, E. C. (2019). Getting to know you: Social media personalization as a means of enhancing brand loyalty. Journal of Retailing and Consumer Services, 47, 57-65. https://doi.org/10.1016/j.jretconser.2018.10.007

Sipos, D. (2024). Harnessing artificial intelligence for hyper-personalization in digital marketing. Technium Business and Management, 9, 47-55. https://doi.org/10.47577/business.v9i.11724

Solberg, E., Kaarstad, M., Eitrheim, M. H. R., Bisio, R., Reegård, K., & Bloch, M. (2022). A conceptual model of trust, perceived risk, and reliance on AI decision aids. Group & Organization Management, 47, 187-222. https://doi.org/10.1177/10596011221081238

Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). Surveillance capitalism. In Ethics of Artificial Intelligence. Springer. https://doi.org/10.1007/978-3-031-17040-9_4

Swani, K., Milne, G. R., & Slepchuk, A. N. (2021). Revisiting trust and privacy concern in marketing information management. Journal of Interactive Marketing, 56, 137-158. https://doi.org/10.1016/j.intmar.2021.03.001

Teraiya, V., & Krishnamurthy, R. (2025, February 4). Balancing personalized marketing and data privacy in the era of AI. California Management Review. https://cmr.berkeley.edu/2025/02/balancing-personalized-marketing-and-data-privacy-in-the-era-of-ai/

Tomar, G., & Pandey, L. (2024). Influence of personalized advertising on consumer engagement and conversion rates [Preprint]. ResearchGate. https://www.researchgate.net/publication/382305674

Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence. Journal of Business Research, 186, 115010. https://doi.org/10.1016/j.jbusres.2024.115010

Yadav, T., Kala, K., Kolachina, R., Kanneganti, M., & Pasupuleti, S. (2024). Data privacy concerns and their impact on consumer trust. International Journal of Scientific Research in Engineering and Management, 8, 1-7. https://doi.org/10.55041/IJSREM38555

Zhu, H., Ou, C., Heuvel, W. J. A. M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce. Information & Management, 54. https://doi.org/10.1016/j.im.2016.10.001