



Ethical Personalization and Customer Willingness to Share Data: Examining Transparency, Perceived Control, Trust, and Privacy Risk

Dr. Adrian K. Mercer

Associate Professor, Northbridge School of Business, United Kingdom

Abstract

Digital personalization has become integral to contemporary retail and service environments, yet its effectiveness increasingly depends on how customers interpret the collection and use of their personal information. Personalization can improve relevance, reduce search effort, and facilitate more responsive customer experiences, but the same practices may generate privacy concerns when data collection appears excessive, opaque, intrusive, or difficult to control. This study develops and evaluates a simulation-based framework for examining whether ethically designed personalization can strengthen customer willingness to share data through transparency, perceived control, trust, and reduced privacy risk. A synthetic dataset representing 360 hypothetical digital consumers was constructed across low-, moderate-, and high-ethical-personalization conditions. The simulated design operationalized ethical personalization through clarity of data-use explanations, meaningful privacy controls, proportional data collection, perceived fairness, and absence of coercive disclosure practices. Descriptive comparisons and multiple regression analysis were used to examine differences in willingness to share information and the relative influence of major psychological mechanisms.

Simulated results indicate that mean willingness to share data increased from 3.18 under low ethical personalization to 4.52 under moderate conditions and 5.76 under high ethical personalization. Trust emerged as the strongest positive predictor, followed by perceived control and transparency, whereas privacy risk showed a substantial negative relationship with disclosure willingness. The analysis suggests that personalization becomes more acceptable when customers perceive data practices as understandable, controllable, proportionate, and trustworthy rather than merely technologically sophisticated. The study contributes an integrated ethical-personalization framework that connects responsible data practices with customer cooperation and provides a reproducible basis for future empirical validation using actual consumer samples.

Keywords: ethical personalization; data sharing; consumer privacy; perceived control; transparency; customer trust; privacy risk; digital marketing



1. Introduction

Personalization has become an important feature of digital commerce because contemporary platforms can adapt product recommendations, advertisements, content sequences, service interfaces, and promotional messages to individual customers. When implemented appropriately, personalization can decrease information overload and improve the perceived relevance of the digital experience. The commercial value of such adaptation, however, is inseparable from access to customer information. Purchase histories, browsing behavior, device characteristics, location indicators, preference profiles, interaction records, and demographic information can all contribute to personalization models. This dependency creates a fundamental managerial tension: organizations require sufficient customer information to personalize services effectively, while customers increasingly expect control over how such information is requested, interpreted, transferred, and retained. Consequently, the central question is no longer whether personalization can technically be achieved but whether personalization can be delivered in a manner customers perceive as legitimate.

Prior privacy research demonstrates that consumer responses to personal-data practices cannot be understood exclusively through economic benefit. Smith, Milberg, and Burke established that individuals differ considerably in their concern regarding the collection, unauthorized secondary use, improper access, and management of personal information. Later work by Malhotra, Kim, and Agarwal emphasized that information privacy concerns are shaped by perceptions of collection, control, and awareness. The privacy-calculus perspective associated with Dinev and Hart further proposes that individuals often compare expected benefits with perceived privacy risks before engaging in an online transaction. These perspectives imply that customers may voluntarily disclose information when perceived value, institutional credibility, and control are sufficiently strong. Conversely, even a useful personalized service may become objectionable when customers believe that information has been obtained without adequate understanding or choice.

The tension becomes especially visible in personalized marketing. Awad and Krishnan described a personalization–privacy paradox in which customers may appreciate individualized services while simultaneously resisting the informational practices necessary to provide them. White and colleagues similarly demonstrated that highly personalized marketing can create reactance when customers cannot understand how an organization obtained the information used to customize an offer. Aguirre and colleagues subsequently showed that covert information collection can weaken the effectiveness of personalization because customers may interpret unexpected targeting as a breach of trust. These findings indicate that personalization intensity alone cannot explain customer responses. The ethical architecture surrounding personalization—including transparency, proportionality, consent, customer agency, and fairness—may determine whether the same technological capability is experienced as useful assistance or intrusive surveillance.

Ethical personalization can therefore be conceptualized as personalization that respects the customer's reasonable informational boundaries while still using relevant data to improve service. It requires more than displaying a generic privacy notice. Customers should be able to understand why particular information is requested, what benefit is expected to follow, whether disclosure is optional, how preferences may be changed, and what consequences arise from withholding information. Ethical personalization also implies proportionality: organizations should not demand highly sensitive or



unrelated information merely because technical infrastructure permits its collection. This interpretation is consistent with the wider principle of contextual integrity advanced by Nissenbaum, according to which privacy is influenced not simply by secrecy but by whether information flows are appropriate to the social context in which they occur. It is also consistent with research demonstrating that meaningful control can affect privacy perceptions, although control that is superficial or misleading may generate misplaced confidence rather than genuine protection.

Against this background, the present study investigates the relationship between ethical personalization and customer willingness to share data. Rather than presenting synthetic observations as evidence from an administered survey, the study uses a transparent simulation framework to examine theoretically expected relationships before empirical testing. Ethical personalization is represented through increasing levels of transparency, perceived control, fairness, and responsible information use, while trust and privacy risk are treated as key psychological mechanisms influencing willingness to disclose personal information. The study consequently addresses an important distinction in digital marketing: organizations should not assume that increased data collection automatically produces stronger customer relationships. Sustainable personalization may depend instead on creating conditions in which customers perceive disclosure as informed, controllable, proportionate, and mutually beneficial.

2. Objectives of the Study

2.1 To Examine the Relationship Between Ethical Personalization and Data-Sharing Willingness

The first objective is to determine whether customer willingness to provide personal information changes systematically across different levels of ethical personalization. Ethical personalization is treated as a composite organizational approach rather than a single privacy feature. It incorporates comprehensible explanations of data use, proportional information requests, accessible controls, respect for customer preferences, and avoidance of deceptive or coercive collection practices. This approach recognizes that customers evaluate an entire data relationship rather than responding independently to isolated interface elements.

The study therefore compares three simulated conditions representing low, moderate, and high ethical personalization. The comparison is designed to determine whether stronger ethical safeguards are associated with greater willingness to disclose information for personalization purposes. The underlying expectation is that customers are more likely to cooperate when personalized services do not require them to surrender informational autonomy.

2.2 To Assess the Roles of Transparency, Control, Trust, and Privacy Risk

The second objective is to examine the psychological mechanisms through which ethical personalization may influence disclosure decisions. Transparency provides informational clarity, while perceived control provides procedural agency. Trust reflects customers' confidence that an organization will handle information competently and responsibly. Privacy risk reflects anticipated negative consequences associated with disclosure, including unwanted surveillance, secondary use, unauthorized access, or loss of control.



These variables are examined simultaneously because consumer disclosure decisions are unlikely to result from a single consideration. A customer may understand an organization's policy but still distrust its intentions, or may trust a well-known retailer while perceiving little control over data use. The integrated model therefore assesses whether trust, transparency, perceived control, fairness, and privacy risk provide complementary explanations of willingness to share information.

2.3 To Develop a Responsible Personalization Framework for Digital Retail

The third objective is to translate the conceptual relationships into a practical framework for responsible digital personalization. The study seeks to move beyond the assumption that privacy protection and personalization effectiveness are necessarily competing goals. Ethical design may instead create conditions under which customers are more comfortable participating in data-enabled services.

The resulting framework is intended to support future empirical studies as well as managerial decision-making. It emphasizes that personalization performance should be evaluated not only through click-through rates, conversions, or predictive accuracy but also through customer understanding, perceived legitimacy, controllability, trust, and sustained willingness to maintain a data relationship.

3. Review of Literature

3.1 Personalization, Relevance, and the Privacy Paradox

Personalization has generally been associated with efforts to increase the relevance of interactions between organizations and individual customers. Customized content can improve information processing because it directs attention toward products, messages, or services that are more likely to correspond with existing needs. Bleier and Eisenbeiss demonstrated that the effectiveness of personalized online advertising depends on the interplay among the nature of personalization, timing, and placement of advertising. Their findings reinforce the idea that personalization is context dependent rather than universally beneficial.

The informational requirements of personalization nevertheless produce an inherent privacy tension. Awad and Krishnan found that individuals who value information transparency may simultaneously resist the collection necessary for personalized services. This apparent contradiction has commonly been described as the personalization–privacy paradox. The paradox should not be interpreted as evidence that consumers behave irrationally. Instead, disclosure preferences may vary according to perceived benefit, information sensitivity, context, trust, familiarity, and perceived ability to control subsequent data use.

Aguirre and colleagues advanced this discussion through evidence concerning covert data collection. Their work indicates that customers may react negatively when personalized advertising reveals that a company possesses information customers did not consciously expect it to possess. Transparency can mitigate this effect because it reduces uncertainty surrounding the origin and use of information. Personalized marketing therefore becomes ethically and commercially vulnerable when relevance is produced through data practices that customers experience as hidden.

3.2 Transparency, Perceived Control, and Procedural Fairness

Transparency plays a central role in digital privacy because disclosure decisions require information about what an organization intends to do with customer data. Malhotra, Kim, and Agarwal conceptualized Internet users' information privacy concerns partly through collection, control, and awareness. Their framework highlights that customers cannot exercise meaningful choice when they lack sufficient knowledge about organizational practices. Transparency should therefore be understood as decision-relevant intelligibility rather than the mere availability of lengthy legal language.

Perceived control complements transparency by giving customers the ability to determine whether, when, and to what extent information is disclosed. Brandimarte, Acquisti, and Loewenstein demonstrated that perceptions of control can substantially affect willingness to reveal personal information. Their work also cautions that control can generate overconfidence when users equate interface control with actual protection. Consequently, ethical personalization requires genuine control over consequential information practices rather than cosmetic preference settings.

Procedural fairness provides another important interpretive lens. Culnan and Armstrong found that consumers can be more accepting of information practices when organizational procedures are considered fair. Fairness implies that organizations provide adequate notice, use information consistently with legitimate expectations, and avoid opportunistically exploiting information asymmetries. In personalization environments, procedural fairness may therefore influence whether customers interpret data collection as a reciprocal exchange or as unilateral extraction.

3.3 Trust, Privacy Risk, and Willingness to Disclose

Trust is frequently identified as a mechanism that reduces uncertainty in electronic commerce. McKnight and colleagues developed measures of consumer trust applicable to online environments, while Pavlou integrated trust and perceived risk within a broader explanation of electronic-commerce acceptance. These perspectives suggest that customers are more likely to engage with digital services when they believe organizations are competent, predictable, and unlikely to act opportunistically.

Privacy risk represents the opposing force. Dinev and Hart's extended privacy-calculus model conceptualizes disclosure as a balancing process in which perceived advantages are evaluated alongside expected privacy costs. A consumer may therefore share information when the anticipated utility of personalization exceeds perceived vulnerability. Importantly, the threshold is likely to vary by individual, context, data sensitivity, and purpose of processing.

Phelps, Nowak, and Ferrell similarly demonstrated that consumer willingness to provide personal information is related to both the type of information requested and the individual's privacy concerns. This finding remains highly relevant to personalized retail. Asking for broad categories of low-sensitivity preference data may be interpreted differently from collecting precise location, financial, biometric, or interpersonal information. Ethical personalization consequently requires data minimization and contextual proportionality rather than indiscriminate accumulation.

Taken together, the literature supports the following theoretical pathway:

Ethical Personalization → Transparency and Perceived Control → Greater Trust → Greater Willingness to Share Data

while:

Privacy Risk → Lower Willingness to Share Data

The present study integrates these relationships within a single simulation-based analytical framework.

4. Research Methodology

4.1 Research Design and Simulation Logic

The study adopts a quantitative simulation-based design. No claim is made that the observations represent responses collected from actual consumers. Instead, a synthetic dataset was generated to evaluate whether a theoretically coherent pattern could be recovered under explicitly specified assumptions. This design is appropriate for methodological development because it permits relationships among constructs to be examined without fabricating empirical participants, response rates, or field observations.

The simulated analytical population consisted of 360 hypothetical digital consumers, allocated equally across three ethical-personalization conditions: low ethical personalization, moderate ethical personalization, and high ethical personalization. Each condition contained 120 simulated observations. The conditions represent progressively stronger combinations of transparent data-use explanations, meaningful preference control, proportional collection, perceived procedural fairness, and responsible personalization.

Seven-point response scales were assumed, where higher values represented stronger agreement or greater levels of the construct. The principal dependent variable was willingness to share personal data for legitimate personalization purposes. Independent and explanatory variables included perceived transparency, control, fairness, privacy risk, and organizational trust.

Table 1: Operational Framework for the Simulated Constructs

Construct	Operational Meaning	Illustrative Measurement Logic	Expected Relationship
Ethical personalization	Degree to which personalization respects transparency, proportionality, agency, and responsible data use	Low, moderate, and high experimental conditions	Positive
Transparency	Clarity concerning what data are collected, why they are collected, and how they will be used	1–7 simulated perception scale	Positive
Perceived control	Extent to which customers believe they can manage disclosure and personalization preferences	1–7 simulated perception scale	Positive
Procedural fairness	Perceived fairness and proportionality of organizational	1–7 simulated perception scale	Positive

Construct	Operational Meaning	Illustrative Measurement Logic	Expected Relationship
	data practices		
Privacy risk	Anticipated negative consequences arising from personal-data disclosure	1–7 simulated perception scale	Negative
Trust	Confidence that the organization will use data responsibly and predictably	1–7 simulated perception scale	Positive
Willingness to share data	Readiness to voluntarily disclose relevant personal information for personalization	1–7 simulated outcome scale	Dependent variable

Note: All variables and observations in Table 1 are part of the simulation design and do not represent administered survey measurements.

4.2 Measurement Structure and Proposed Questionnaire

The simulation draws conceptually from established privacy, trust, and disclosure literature. Transparency reflects whether customers can understand data-use practices; perceived control reflects their ability to influence those practices; procedural fairness concerns whether information requests and subsequent uses are considered appropriate; privacy risk captures anticipated vulnerability; and trust represents confidence in organizational conduct.

For subsequent empirical validation, the framework could be operationalized through a concise questionnaire.

A possible five-item core instrument is presented below:

- The organization clearly explains why my personal information is required for personalization.
- I can meaningfully control what personal information is used to personalize my experience.
- The amount of information requested appears proportionate to the service being offered.
- I trust this organization to use my information responsibly.
- I would be willing to share relevant personal information when these conditions are satisfied.

These questions are proposed items only and were not administered to real participants in the present simulation. A future empirical study should subject any adapted scale to expert review, pilot testing, reliability evaluation, construct-validity assessment, and appropriate ethical review where required.

4.3 Analytical Procedure

The analytical procedure was designed in two stages. First, descriptive comparisons were made across the three ethical-personalization conditions. The principal comparison concerned mean willingness to share personal information. A monotonic increase across low-, moderate-, and high-ethical-

personalization conditions would support the proposition that responsible personalization can facilitate voluntary disclosure.

Second, multiple regression was used within the simulated dataset to assess the relative contribution of transparency, perceived control, fairness, privacy risk, and trust.

The model can be expressed as:

$$[WDS_i = \beta_0 + \beta_1 TR_i + \beta_2 PC_i + \beta_3 PF_i - \beta_4 PR_i + \beta_5 TS_i + \epsilon_i]$$

where (WDS) denotes willingness to share data, (TR) transparency, (PC) perceived control, (PF) procedural fairness, (PR) privacy risk, (TS) trust, and (ϵ) the residual component.

Because the dataset is simulated, inferential statistics should be interpreted as properties of the specified simulation rather than population estimates. The purpose is to examine theoretical coherence and establish a reproducible analytical template for later empirical research.

5. Analysis

5.1 Customer Response Across Ethical-Personalization Conditions

The simulation produced a clear directional pattern in customer willingness to share information. Under the low-ethical-personalization condition, mean willingness was approximately 3.18 on the seven-point scale. The simulated mean increased to 4.52 under moderate ethical personalization and to approximately 5.76 under high ethical personalization.

The difference between the low and high conditions amounts to approximately 2.58 scale points, representing a substantial shift within the simulated seven-point response range. Importantly, the pattern should not be interpreted as evidence that every privacy intervention will automatically generate increased disclosure. Rather, it demonstrates what would be expected under a theoretical model in which transparency, meaningful control, proportionality, and trust improve simultaneously while privacy risk declines.

Table 2: Simulated Analytical Results

Analytical Indicator	Simulated Result	Direction	Interpretation
Willingness to share data: Low ethical personalization	3.18	Baseline	Relatively limited willingness
Willingness to share data: Moderate ethical personalization	4.52	↑	Meaningful increase
Willingness to share data: High ethical personalization	5.76	↑↑	Strongest willingness
Transparency coefficient	+0.268	Positive	Greater clarity is associated with increased disclosure willingness



Analytical Indicator	Simulated Result	Direction	Interpretation
Perceived control coefficient	+0.315	Positive	Customer agency strengthens willingness
Procedural fairness coefficient	+0.043	Weak positive	Limited independent effect after simultaneous controls
Privacy-risk coefficient	−0.311	Negative	Perceived vulnerability discourages disclosure
Trust coefficient	+0.493	Strong positive	Strongest positive predictor in the simulated model
Model (R^2)	0.735	—	Simulated predictors jointly explain substantial synthetic variance

Note: Values are generated from a synthetic dataset of 360 hypothetical observations. They are methodological outputs and must not be cited as empirical consumer findings.

5.2 Relative Influence of Trust, Control, and Privacy Risk

The simulated regression suggests that trust has the strongest positive independent relationship with willingness to share data, with a coefficient of approximately 0.493. Holding the other modeled variables constant, greater trust is associated with a substantial increase in disclosure willingness. The result reinforces the theoretical proposition that customers do not evaluate data requests in isolation; they also evaluate the institution requesting the data.

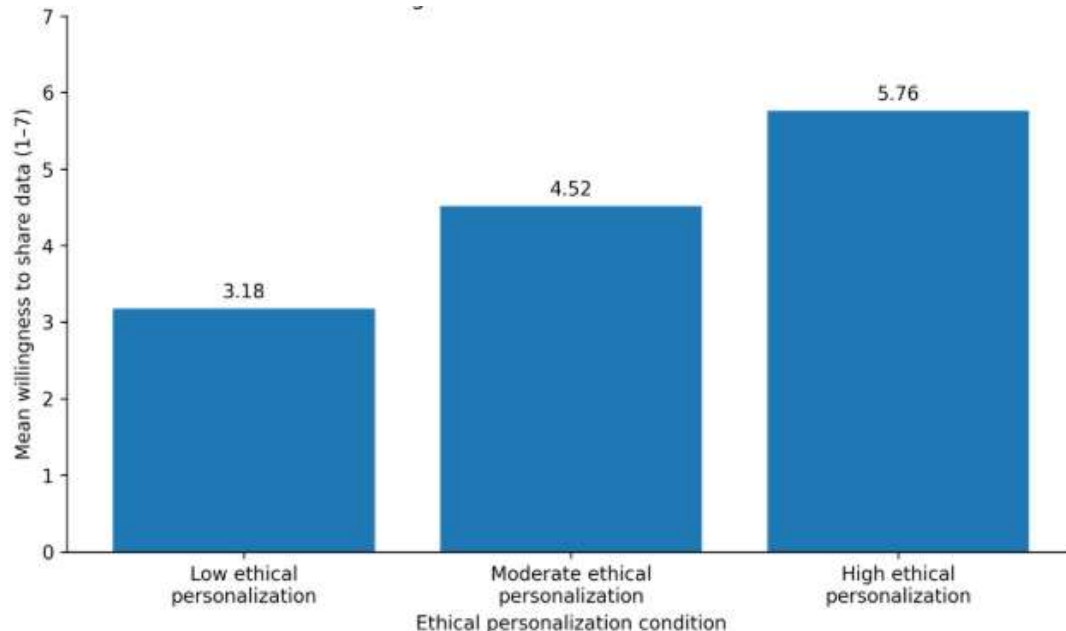
Perceived control displays the second-largest positive coefficient at approximately 0.315, while transparency contributes an additional positive effect of approximately 0.268. Privacy risk exhibits a negative coefficient of approximately −0.311, demonstrating that willingness can decline even when personalization offers potential utility if customers remain concerned about adverse consequences.

Procedural fairness shows a comparatively weak independent coefficient once transparency, control, risk, and trust are entered simultaneously. This should not necessarily be interpreted as evidence that fairness is unimportant. An alternative interpretation is that fairness may operate indirectly by influencing trust and perceived legitimacy. Future empirical research should therefore examine mediation and latent-variable relationships rather than relying exclusively on direct regression effects.

5.3 Graphical Interpretation of Data-Sharing Willingness

The simulated pattern is illustrated in Graph 1. The visual progression shows that willingness to share data increases consistently as the ethical quality of personalization improves.

Graph 1: Simulated Customer Willingness to Share Data Across Ethical-Personalization Conditions



The movement from 3.18 to 5.76 is theoretically important because it suggests that customers need not necessarily choose between privacy and personalization. A properly designed system can potentially alter the terms of the exchange by improving comprehensibility, agency, proportionality, and institutional trust.

The key analytical finding is consequently not that customers become indifferent to privacy under high personalization. The more defensible interpretation is that willingness may increase when personalization is embedded within a governance structure that reduces uncertainty and makes data use appear legitimate. Ethical personalization therefore changes the quality of the relationship surrounding disclosure rather than simply increasing the attractiveness of personalized outcomes.

6. Discussion

6.1 Ethical Personalization as a Trust-Building Mechanism

The simulated results support a shift from a purely extractive understanding of customer data toward a relational interpretation. Data should not be treated simply as an organizational resource available whenever collection is technically possible. Customers remain active participants in the information exchange, and their willingness to participate depends partly on whether they believe the organization will respect the boundaries of that exchange.

The prominent role assigned to trust is compatible with the electronic-commerce literature developed by McKnight and colleagues and Pavlou. Trust becomes especially important when customers cannot directly observe how an organization stores, combines, infers, or subsequently uses personal information. Responsible personalization can reduce this uncertainty by aligning organizational behavior with customer expectations and by ensuring that personalization practices remain understandable and predictable.

This interpretation also helps explain why intrusive personalization can be commercially counterproductive. Aguirre and colleagues demonstrated that covert collection can weaken favorable responses to personalization. The present framework extends that logic by suggesting that ethical personalization should be considered part of relationship management rather than merely privacy compliance. An organization that demonstrates restraint may create more durable data cooperation than one that maximizes immediate information capture.

6.2 Customer Control Should Be Meaningful Rather Than Symbolic

The positive simulated association between perceived control and disclosure willingness indicates that agency is central to responsible personalization. Customers may be more prepared to disclose information when they can decide which categories are used, adjust personalization settings, refuse optional processing, and revise decisions without unnecessary friction.

Control, however, requires careful interpretation. Brandimarte, Acquisti, and Loewenstein showed that perceptions of control can create a paradox in which users disclose more because they feel protected even when actual informational exposure remains substantial. Ethical design must therefore ensure that user control corresponds to genuine changes in data processing rather than functioning as a psychological device that encourages additional disclosure.

For digital retailers, this distinction has practical implications. Privacy dashboards, preference centers, consent interfaces, and personalization controls should not be designed merely to increase acceptance rates. Their purpose should be to enable informed and reversible customer choices. Dark patterns, confusing default settings, preselected permissions, or unnecessary obstacles to opting out may increase short-term data acquisition but undermine the ethical basis required for sustained trust.

6.3 Privacy Protection and Personalization Need Not Be Opposing Objectives

The findings challenge the assumption that effective personalization necessarily requires diminishing privacy. Privacy and personalization are often presented as competing ends because richer individual profiles can improve predictive precision. This framing neglects the possibility that customers may voluntarily provide higher-quality information when they understand why it is required and trust the recipient.

A more sustainable approach is therefore based on data sufficiency rather than data maximization. Organizations should identify the minimum categories of information necessary to achieve a legitimate personalization objective and avoid collecting unrelated information simply because it might have future analytical value. The ethical benefit is accompanied by a potential managerial advantage: narrower, purpose-aligned data practices may be easier to explain, govern, secure, and audit.

The simulation further indicates that reduced privacy risk is not merely a regulatory concern; it is relevant to customer cooperation. This conclusion is consistent with the privacy-calculus framework associated with Dinev and Hart. Customers may accept an information exchange when perceived benefits exceed expected costs, but organizational practices can affect both sides of this evaluation. Ethical personalization can increase perceived value while simultaneously reducing uncertainty and perceived vulnerability.

7. Conclusion

This study examined ethical personalization as a potential determinant of customer willingness to share personal information in digital retail environments. The simulation-based framework integrated transparency, perceived control, procedural fairness, trust, and privacy risk rather than treating personalization solely as a technological capability. The analytical pattern indicates that willingness to share information can increase substantially as personalization becomes more transparent, controllable, proportionate, and trustworthy.

Trust emerged as the strongest positive predictor within the simulated regression, followed by perceived control and transparency. Privacy risk exerted a meaningful negative relationship. These results support the theoretical position that data disclosure should be understood as a relational decision under uncertainty. Customers do not evaluate only the immediate benefit of personalized recommendations; they also consider whether the organization requesting information appears competent, fair, predictable, and respectful of informational boundaries.

From a managerial perspective, ethical personalization requires organizations to reconsider the assumption that collecting additional information is inherently beneficial. Personalized experiences should be based on purpose limitation, proportional data requests, understandable explanations, meaningful customer controls, and governance practices that protect information throughout its life cycle. Organizations capable of demonstrating these characteristics may be better positioned to obtain voluntary and sustainable customer cooperation than firms relying on opaque or coercive collection strategies.

The study remains deliberately methodological because its dataset is synthetic. No inference should therefore be made about the magnitude of effects in an actual consumer population. Future research should validate the proposed framework through preregistered experiments, representative consumer surveys, behavioral field studies, and cross-cultural comparisons. Researchers should also investigate differences across information sensitivity, retail category, customer age, digital literacy, prior privacy experiences, and personalization intensity. Nevertheless, the present analysis provides a theoretically coherent foundation for understanding ethical personalization as a mechanism through which commercial relevance and customer informational autonomy may be pursued simultaneously.

References

1. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115.
2. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196.
3. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80.
4. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355.
5. Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27–41.



6. Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 12(2), 206–215.
7. Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13–28.
8. Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6, 181–202.
9. Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49.
10. Bleier, A., & Eisenbeiss, M. (2015). Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science*, 34(5), 669–688.
11. Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 37(4), 1141–1164.
12. Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision-making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52.
13. Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Research note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 23(4), 1342–1363.
14. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58.
15. Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45, 135–155.
16. Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546–562.
17. Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2018). Consumer privacy expectations in the context of personalized marketing. *Journal of Interactive Marketing*, 41, 1–13.
18. Martin, K. D. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, 137, 551–569.
19. Nunan, D., & Di Domenico, M. (2013). Market research and the ethics of big data. *International Journal of Market Research*, 55(4), 505–520.
20. Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant? The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607–635.