Consumer Trust in the Artificial Intelligence Era: Influence of Data Protection Practices on Purchase Intention

Kutlu Ergün
Balıkesir University, Faculty of Economics and Administrative Sciences, Balıkesir, Türkiye
kutlu.ergun@balikesir.edu.tr

This paper examines how data protection practices function as early indicators of trust and governance mechanisms in AI-driven, data-intensive digital markets. Within the digital economy, data-driven value creation through personalization, segmentation, and relationship management amplifies privacy and risk concerns, which subsequently influence the evolution of trust. Effective data protection and transparent communication are identified as critical determinants of market value. While structural cues are initially prominent, the website experience gains importance as user interactions progress. The expansion of data processing and sharing in AI environments further highlights the necessity of maintaining privacy balances. This article clarifies the essential role of open and standardized privacy communication in fostering consumer trust and enhancing market value, and discusses implications for marketing, policy, and future research. This study integrates previously fragmented discussions on privacy assurance, personal data control, transparency, perceived risk, and purchase intention into a concise conceptual framework. This framework explains how data protection practices function as trust-building mechanisms in AI-driven digital markets.

DOI
https://doi.org/10.18690/um.epf.7.2026.65

ISBN
978-961-299-166-1

Keywords:
consumer trust, data protection, privacy assurance, AI-driven markets, purchase intention

JEL:
M31, D83, L86

University of Maribor Press

1 Introduction

Within the digital economy, organizations generate value through personalization, segmentation, and relationship management, all of which depend on customer data. Although data-driven value creation offers advantages to consumers, it also increases perceptions of uncertainty and risk, thereby emphasizing the critical role of trust. Trust in online environments is dynamic and develops throughout the decision-making process. As this process unfolds, the cues influencing trust formation may change. Research demonstrates that structural trust indicators are most influential during the initial stages of decision making, whereas factors related to the website experience become more prominent as user interaction continues (McKnight et al., 2004). In this context, data protection practices function as early indicators of trust that inform consumers' trust assessments. The effectiveness of these practices, however, is contingent upon both the specific context and the manner in which they are communicated during the decision-making process.

In the age of artificial intelligence, the increasing data processing capacity is raising uncertainties regarding the collection, processing, and sharing of consumer data. This development necessitates balancing benefits with privacy concerns in consumer interactions with data-driven services. Consumers need clear, comparable information to assess data protection assurances effectively. Research on the privacy label approach developed under the General Data Protection Regulation (GDPR) reveals that current practices often fail to improve consumers' perceptions of privacy and control. Conversely, more transparent and standardized information presentations can increase perceived levels of control, privacy, and trust (Fox et al., 2022). Therefore, the fundamental challenge in the context of artificial intelligence is to go beyond data processing and ensure that these processes are understandable, traceable, and manageable from a consumer perspective.

Data protection practices foster trust in marketing and indicate responsible data management. However, trust is influenced not only by these practices but also by consumers' awareness and comprehension of them during decision-making. When privacy information is made available, research demonstrates that consumers prefer options with stronger privacy protection and are willing to pay a premium for such options (Tsai et al., 2011). While data protection entails compliance costs, it also generates market value. The effectiveness of trust signals varies; certain third-party

signals do not enhance consumer trust (McKnight et al., 2004). Therefore, data protection communication should employ clear and easily understandable signals for consumers. This paper contributes to the literature by conceptualizing data protection practices as both regulatory requirements and early-stage trust signals in AI-driven consumer markets. It integrates privacy assurance, perceived control, transparency, perceived risk, and purchase intention into a unified conceptual framework. This discussion-oriented framework is intended to inform future empirical research on consumer evaluation of data protection practices during purchasing decisions in data-intensive digital environments.

2 Literature review

2.1 Consumer Trust in AI-Driven Digital Environments

Trust is widely recognized as a critical determinant in digital environments, especially within e-commerce, due to the virtual nature of transactions and the absence of direct interpersonal interaction. According to Habib and Hamadneh (2021), trust holds greater significance in online shopping than in traditional transactions and serves as a fundamental factor in the adoption of new technologies and the expansion of e-commerce. The same study further demonstrates that trust is positively correlated with technical security features, ease of site navigation, information presentation, and verification.

Within this framework, consumer trust functions as a mechanism closely linked to perceived risk and uncertainty. Habib and Hamadneh (2021) assert that consumers often perceive online shopping as risky, with "fear of the unknown" identified as a primary barrier to online purchasing. The same study suggests that perceived risk is assessed in relation to the "subjective ambiguity" of potential outcomes. Similarly, Hipólito et al. (2025) find that consumer trust in online shopping environments reduces perceived risk and consequently enhances satisfaction with the shopping experience. Their research also observes that businesses implement return policies to mitigate consumer uncertainty. However, the effect of a free return option on risk perception and satisfaction may be less substantial than anticipated, while an open return policy can lead to increased satisfaction. Additionally, a non-linear relationship is proposed between risk perception and satisfaction, indicating that satisfaction may peak at an optimal level of risk, forming an inverse U-shaped

relationship. In digital contexts, trust is evaluated not only in terms of confidence in technology or online systems but also through trust beliefs related to firms' data collection practices. Addressing the personalization-privacy paradox, Cloarec et al. (2024) emphasize the tension between the desire for personalized experiences and the need to protect personal data, defining trust beliefs and concerns about information collection as central components of their models.

2.2 Data Protection Practices as Responsible Data Governance

Fox et al. (2022) demonstrate that GDPR-style visual privacy labels are more effective than lengthy, text-based privacy policies in shaping consumers' privacy perceptions and behaviors within e-commerce. These labels reduce perceived risks and enhance feelings of control, particularly when explicit consent mechanisms are implemented. Increased control and privacy strengthen consumers' perceptions of company trustworthiness, encompassing benevolence, honesty, and competence. This, in turn, elevates purchase intent and willingness to provide accurate data. The authors contend that responsible data management should extend beyond compliance, advocating for transparency and actionable practices that empower user control and foster trust in cross-border regulatory environments.

Zimmermann et al. (2024) conceptualize personal data control as a multi-stage construct comprising four distinct activities in consumer-firm data exchanges: collection, transmission, access, and use. Their findings indicate that consumers can distinguish among these stages, although subjective perceptions of control do not always align with objective behavioral control. When multiple activities occur simultaneously or when active participation is limited, perceptions of collection and transmission may overlap, and some perceptions of data flow may converge. The authors recommend that both research and practice employ comprehensive measurement approaches encompassing all four control activities, as reliance on single-factor measures may distort consumer evaluations in data disclosure contexts. By distinguishing between active, passive, and hybrid disclosure scenarios, the study broadens the discourse on privacy and technology adoption. The authors further assert that control over data inputs in automated and artificial intelligence contexts is a critical management issue rather than solely a technical concern.

Thompson and Siamagka (2022) report that perceptions of ethical care in organizational privacy practices positively influence both perceived information control and trust in the company. These perceptions subsequently shape consumers' information-sharing behaviors. The accuracy of information shared is fully determined by perceived information control and trust, while the quantity of information shared is primarily affected by the direct influence of perceived ethical care. Using structural equation modeling and experimental methods, the authors' model accounts for 18.1% of the variance in the amount of information shared and 37.6% of the variance in willingness to share accurate information, outperforming a regulation-based antecedent model in both fit and explanatory power. The authors conclude that adopting an ethical care governance perspective, rather than relying exclusively on regulations, may mitigate privacy-related issues such as data withholding or falsification and promote more accurate data disclosure by enhancing perceptions of control and trust linked to transparency.

Montecchi et al. (2024) find that perceived brand transparency, conceptualized as a second-order construct, demonstrates strong model fit and discriminant validity within their proposed framework. Structural equation modeling results indicate that perceived brand transparency is strongly and positively associated with key managerial outcomes, including brand credibility, integrity, authenticity, beliefs about corporate social responsibility and ethics, and brand trust. The authors also observe that higher perceived brand transparency correlates with more favorable purchase intentions. The study concludes that transparency strategies can reduce information asymmetry and consumer skepticism, rebuild trust, and foster mutually beneficial, trust-based relationships between brands and consumers.

2.3 Trust and Data-Driven Behavior in AI Environments

The widespread adoption of the internet in Business-to-Consumer commerce has intensified academic focus on firm-customer interactions in online settings. In this context, trust is a fundamental driver of consumer engagement. Elevated trust in e-commerce, alongside substantial web experience, increases the probability of consumers participating in online shopping. Key determinants of trust include perceived market orientation, site quality, technical reliability, and users' web experience. High perceived site quality is particularly associated with stronger market

orientation and reliability. Enhanced trust, in turn, promotes greater engagement in e-commerce (Corbitt et al., 2003).

A trust-based consumer decision model has been introduced to analyze the interplay between trust and risk in online purchasing. According to this model, trust, perceived risk, and perceived benefit each exert direct effects on purchase intentions and decisions. Trust also indirectly influences purchase intention by mitigating perceived risk. Empirical evidence indicates that trust has a strong positive impact on purchase intention, whereas perceived risk reduces it and perceived benefit increases it. These factors also shape actual purchasing behavior. Consumers' perceptions of privacy and security significantly influence both trust and risk, indicating that privacy and security are assessed as distinct constructs in online shopping. While familiarity substantially affects purchase intention and trust, it does not significantly alter perceived risk. Conversely, a predisposition to trust has a notable effect on consumer trust (Kim et al., 2008).

In the context of the attention economy, achieving an effective balance between personalized advertising and consumer privacy remains a considerable challenge. The allocation of consumer attention is a crucial variable in this dynamic. Limitations on attention can hinder online social interactions and restrict consumers' ability to effectively manage their privacy (Cloarec, 2020). The growing implementation of data-driven technologies and algorithms has increased the collection of personal data across digital and physical environments, thereby enhancing companies' ability to monitor and track media users. As a result, perceived surveillance has become a prominent subject in data-driven communication research. The experience of being observed is associated with decreased media usage and may lead to shifts in media consumption behaviors (Segijn et al., 2022; McDonald & Cranor, 2010). To address the lack of a robust measurement tool, Segijn et al. (2022) validated the Perceived Surveillance Scale across multiple datasets, confirming its reliability for assessing perceived surveillance arising from personalization techniques and personalized communication. Findings on construct validity reveal that perceived surveillance is positively correlated with privacy concerns, perceived privacy risk, perceived vulnerability and seriousness, intimidation, surveillance anxieties, and perceived personalization, and negatively correlated with attitudes toward personalization. Unexpectedly, a positive relationship was found between trust in the fair use of personal data and perceived surveillance, which may serve as a coping response to

privacy concerns (Segijn et al., 2022; Hoffmann et al., 2016; Lutz et al., 2020; van Ooijen et al., 2022).

Prior research demonstrates that trust, perceived risk, privacy assurance, transparency, and personal data control are significant determinants of consumer behavior in online environments. However, the literature is fragmented, with some studies emphasizing trust and perceived risk, while others examine privacy labels, transparency, ethical data practices, or perceived surveillance. For example, Fox et al. (2022) report that GDPR-style privacy labels influence consumers' privacy perceptions, perceived control, trust, and behavioral intentions. Zimmermann et al. (2024) propose that personal data control should be understood as a multi-stage construct within technology-mediated contexts. Montecchi et al. (2024) show that perceived brand transparency is associated with favorable brand evaluations, including trust-related outcomes and purchase intentions. Despite these findings, the role of data protection practices as an integrated trust-building mechanism in AI-driven markets remains insufficiently defined.

Another limitation in the literature is the predominant focus on data protection from either a regulatory compliance or consumer privacy perspective. Few studies examine its strategic function as a market signal that can shape perceived trustworthiness and purchase intention. Mattison Thompson and Siamagka (2022) support this perspective by demonstrating that organizational privacy ethical care enhances perceived information control and trust. This research gap is especially relevant in AI-driven environments, where data collection, algorithmic personalization, and automated decision-making increase both the benefits and perceived risks of digital interaction, thereby intensifying the personalization–privacy paradox (Cloarec et al., 2024). Therefore, data protection practices should be conceptualized as governance-based trust cues. When these practices are communicated in a transparent, standardized, and consumer-oriented manner, they can reduce perceived uncertainty, enhance perceived control, and support purchase intention.

3 Methodology

This article contends that data protection practices are essential indicators of trust and function as governance mechanisms within AI-driven digital environments. Adopting an interdisciplinary perspective, it integrates insights from marketing, information systems, digital consumer behavior, and responsible data governance to examine the operation of these mechanisms. The analysis centers on key concepts such as online trust, perceived risk, purchase intention, privacy assurance, personal data control, ethical diligence, brand transparency, the personalization-privacy paradox, and perceived surveillance. Relevant keywords include consumer trust, data protection, GDPR, personal data control, ethical diligence, brand transparency, purchase intention, perceived risk, personalization-privacy paradox, AI-powered marketing, data-driven communication, and surveillance.

This study employs a conceptual and literature-based methodology, aiming to synthesize existing theoretical and empirical findings into a coherent conceptual framework instead of testing causal relationships with primary data. The analysis draws upon prior research in marketing, information systems, consumer behavior, privacy studies, and responsible data governance. These studies facilitate the identification of recurring constructs, relationships, and research gaps concerning data protection, trust formation, perceived risk, perceived control, transparency, and purchase intention. Drawing upon existing literature, this study introduces a conceptual framework that illustrates the role of data protection in fostering trust within digital environments. The article emphasizes the necessity for robust conceptual models, reliable measurement instruments, and empirical evidence to substantiate the relationship among trust, privacy, and consumer behavior. Although primary quantitative data are not presented in this paper, a foundation is established for future empirical validation. The proposed framework can be evaluated through survey-based research, experimental designs, or structural equation modeling. Future studies could examine whether transparent privacy communication enhances perceived control and trust, whether perceived risk mediates the relationship between data protection and purchase intention, and whether AI-driven personalization increases privacy concerns or perceived surveillance.

Proposed Directions for Future Empirical Research

Drawing from the proposed framework, future empirical studies can empirically test the following propositions:

P1. Transparent communication regarding data protection enhances perceived consumer control.

P2. Higher levels of perceived consumer control strengthen consumer trust.

P3. Increased perceived risk diminishes purchase intention.

P4. Greater consumer trust leads to higher purchase intention.

P5. Perceived risk serves as a mediator between data protection practices and purchase intention.

P6. Perceived surveillance can undermine consumer trust when data protection practices lack clarity.

4 Results and Discussion

The literature shows that data protection practices shape consumer purchase intentions through several interconnected mechanisms. Transparent privacy communication and responsible data governance increase perceived control and build consumer trust, while also reducing perceived risk and uncertainty. In AI-driven contexts, personalization and perceived surveillance may intensify privacy concerns, eroding trust if data protection practices are not communicated effectively. Figure 1 demonstrates how these mechanisms are conceptually linked within AI-driven digital markets.

The literature demonstrates that in AI-driven, data-intensive digital markets, data protection practices function as early indicators of trust, enabling consumers to manage uncertainty and perceived risk in online decision-making. Trust assumes a dynamic role throughout this process. Although structural indicators are initially

prominent, the quality of website experience becomes increasingly decisive as user interaction grows (McKnight et al., 2004). The effectiveness of data protection practices is determined not only by their presence but also by the clarity of their communication and the extent of consumer understanding.

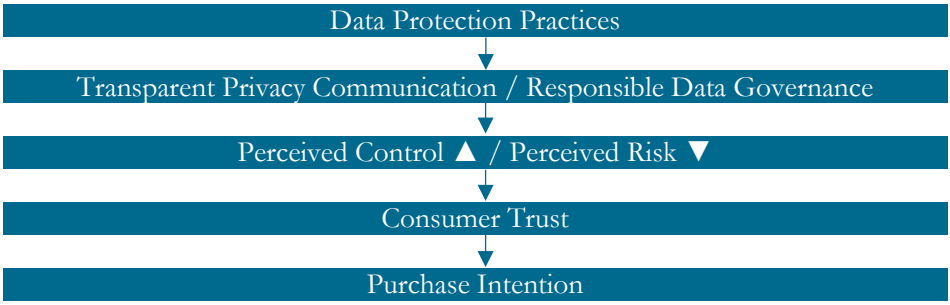

Figure 1: Conceptual Framework of Data Protection, Trust, and Purchase Intention

A critical reading of the literature indicates that the relationship between data protection and trust is not inherently direct. The presence of privacy policies, assurance seals, or formal compliance mechanisms alone may not be sufficient to enhance consumer trust. More significant is the extent to which consumers can understand, compare, and evaluate these practices during their decision-making. This distinction is crucial because certain trust signals may prove ineffective if they are overly complex, merely formally standardized, or disconnected from consumers' actual experiences. Consequently, the effectiveness of data protection relies not only on institutional compliance but also on communicative clarity and the perceived usefulness to consumers.

Within AI environments, increased data processing capacity amplifies uncertainty regarding the collection, processing, and sharing of data. This underscores the necessity of balancing data-driven advantages with privacy concerns. Consumers increasingly require clear and comparable information about data protection assurances. Evidence regarding GDPR-like privacy labels suggests that current practices frequently fail to enhance perceptions of privacy and control. More transparent and standardized presentations may improve perceived control, privacy, and trust (Fox et al., 2022). When privacy information is available, consumers are more likely to prefer and pay for alternatives offering stronger protection. This

outcome indicates that data protection can generate market value despite associated costs (Tsai et al., 2011).

Research indicates that AI-driven data applications contribute to increased uncertainty. Data protection and effective communication emerge as essential governance mechanisms that influence perceived control, privacy, and trust (McKnight et al., 2004; Fox et al., 2022). Trust, in particular, facilitates consumer interaction with digital platforms and correlates with purchasing behavior in social commerce contexts (Wang & Herrando, 2019). Consequently, data protection should be considered not only as a matter of legal compliance but also as an integral component of responsible data management and sustainable governance frameworks. Establishing trust is therefore fundamental to fostering market engagement and generating value.

The literature identifies several areas requiring further empirical investigation. Researchers are encouraged to examine the impact of trust cues at each stage of the decision-making process. It is also necessary to assess whether transparent and standardized privacy communications, such as GDPR-style labeling, enhance perceptions of control, privacy, and trust. Researchers should evaluate how privacy information influences consumer preferences and willingness to pay. Findings suggest that marketers should provide clear, comparable, and comprehensible privacy assurances. Since not all trust signals are equally effective, policymakers are advised to promote disclosures that render data practices transparent, traceable, and manageable for consumers.

5 Conclusion

This study demonstrates that in AI-driven, data-intensive digital markets, data protection practices foster trust by reducing uncertainty and risk in consumers' online decision-making. The effectiveness of data protection depends not only on its implementation but also on the clarity and comprehensibility of its communication. Extensive data processing, collection, and sharing in AI contexts present significant concerns. Transparent and standardized privacy information is essential for enhancing perceived control, privacy, and trust. Effective data protection requires both regulatory compliance and responsible data management, as well as sustainable governance to promote consumer engagement and value

creation. Future research should investigate the influence of trust cues on decision-making and assess how privacy communication affects consumer preferences and willingness to pay. Policy initiatives should emphasize consumer-oriented, clear, and comparable privacy assurances.

The present study is limited by its conceptual and literature-based approach. Therefore, empirical validation of the proposed relationships is required in subsequent research. Future quantitative studies should examine the effects of privacy assurance, perceived control, perceived risk, and consumer trust on purchase intention. Furthermore, experimental research may compare different forms of privacy communication, such as traditional privacy policies, visual privacy labels, and AI-specific transparency notices. Such investigations would help determine which data protection signals most effectively enhance consumer trust in AI-driven markets.

References

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. Technological Forecasting and Social Change, 161, 120299. https://doi.org/10.1016/j.techfore.2020.120299

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization–privacy paradox on social media. Psychology & Marketing, 41(7), 1574–1596. https://doi.org/10.1002/mar.21998

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. Electronic Commerce Research and Applications, 2(3), 203–215. https://doi.org/10.1016/S1567-4223(03)00024-3

Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing perceptions of privacy and trust: A GDPR label perspective. Information Technology & People, 35(8), 181–204. https://doi.org/10.1108/ITP-09-2021-0706

Habib, S., & Hamadneh, N. N. (2021). Impact of perceived risk on consumers technology acceptance in online grocery adoption amid COVID-19 pandemic. Sustainability, 13(18), 10221. https://doi.org/10.3390/su131810221

Hipólito, F., Dias, Á., & Pereira, L. (2025). Influence of Consumer Trust, Return Policy, and Risk Perception on Satisfaction with the Online Shopping Experience. *Systems*, *13*(3), 158. https://doi.org/10.3390/systems13030158

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy Cynicism: A new Approach to the Privacy Paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(4), Article 7. https://doi.org/10.5817/CP2016-4-7

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168-1187. https://doi.org/10.1177/1461444820912544

Mattison Thompson, F., & Siamagka, N.-T. (2022). Counteracting consumer subversion: Organizational privacy ethical care as driver of online information sharing. Psychology & Marketing, 39, 579–597. https://doi.org/10.1002/mar.21579

McDonald, A. M., & Cranor, L. F. (2010). Americans' attitudes about internet behavioral advertising practices. In Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society (WPES '10) (pp. 63–72). https://doi.org/10.1145/1866919.1866929.

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business. Electronic Markets, 14(3), 252–266.

Montecchi, M., Plangger, K., West, D., & de Ruyter, K. (2024). Perceived brand transparency: A conceptualization and measurement scale. Psychology & Marketing, 41(10), 2274–2297. https://doi.org/10.1002/mar.22048

Segijn, C. M., Opree, S. J., & van Ooijen, I. (2022). The validation of the Perceived Surveillance Scale. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 16(3), Article 9. https://doi.org/10.5817/CP2022-3-9

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information systems research, 22(2), 254-268. https://doi.org/10.1287/isre.1090.0260

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy Cynicism and its Role in Privacy Decision-Making. Communication Research, 51(2), 146-177. https://doi.org/10.1177/00936502211060984

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials?. International Journal of Information Management, 44, 164-177. https://doi.org/10.1016/j.ijinfomgt.2018.10.016

Zimmermann, J., Martin, K. D., Schumann, J. H., & Widjaja, T. (2024). Consumers' multistage data control in technology-mediated environments. International Journal of Research in Marketing, 41(1), 56-76. https://doi.org/10.1016/j.ijresmar.2023.09.004