

Fostering Trust and Loyalty in E-Commerce through Ethical Data Practices

Rhea Natania Menaisa Sebayang¹, Tiara Rizky Cahya², Nurhidayah Yahya³, Rafidah Zainal⁴

¹Universitas Lampung, Indonesia

²Universitas Lampung, Indonesia

³Accounting Research Institute, Universiti Teknologi MARA, Shah Alam, Malaysia

⁴Universiti Teknologi MARA, Shah Alam, Malaysia

DOI: <https://doi.org/10.51583/IJLTEMAS.2026.150600219>

Received: 01 July 2026; Accepted: 06 July 2026; Published: 25 July 2026

ABSTRACT

This conceptual paper examines how ethical data practices foster consumer trust and loyalty in e-commerce, with particular emphasis on data privacy, data security, and consumer perceived risk. As digital platforms increasingly depend on personal and behavioural data for personalisation, payment processing, targeted marketing, and customer engagement, consumer concerns regarding transparency, informed consent, unauthorised data sharing, cybersecurity, and manipulative data use have become central to online exchange relationships. Drawing on Social Exchange Theory, the paper proposes that consumers are more willing to maintain relationships with e-commerce platforms when the exchange of personal data for convenience and personalised services is perceived as fair, beneficial, secure, and trustworthy. The paper distinguishes ethical data governance from regulatory compliance by arguing that lawful data processing represents only a minimum threshold, whereas ethical governance also requires fairness, proportionality, accountability, respect for autonomy, and consideration of consumer wellbeing. An integrated conceptual framework is developed in which ethical data practices strengthen consumer loyalty through consumer trust, while perceived privacy and security risk weakens the positive relationship between ethical data practices and trust. The discussion also considers emerging governance challenges associated with generative artificial intelligence, algorithmic personalisation, blockchain, and decentralised identity systems. The paper contributes to e-commerce and business ethics literature by explaining how, and under what conditions, responsible data governance supports sustainable digital relationships. Practical implications are presented for managers, marketers, IT teams, policymakers, and consumers, together with measurable constructs and empirical testing directions for future research.

Keywords: Ethical Data Practices, Data Privacy, Data Security, Consumer Perceived Risk, Consumer Trust, Consumer Loyalty, E-Commerce

INTRODUCTION

The rapid expansion of e-commerce has transformed the way businesses interact with consumers by increasing convenience, personalisation, and global market access. At the beginning of 2025, approximately 5.56 billion people used the internet and 5.78 billion used mobile phones worldwide (DataReportal, 2025). This extensive digital participation has made online platforms a routine part of purchasing behaviour and has increased firms' reliance on browsing histories, payment information, location data, product preferences, and engagement patterns. Although these data support service improvement and personalised experiences, their collection and use also expose consumers to privacy loss, profiling, data breaches, unauthorised sharing, and other forms of misuse.

In e-commerce, privacy, security, and perceived risk are closely connected. Data privacy concerns whether consumers understand and control how their information is collected, processed, stored, and shared, while data

security concerns the safeguards used to protect that information from unauthorised access, loss, or disclosure. Perceived risk arises when consumers believe that an online transaction may result in identity theft, payment fraud, unwanted profiling, data misuse, or loss of control. Because consumers typically disclose personal and financial information before receiving a product or service, trust in online commerce depends substantially on how platforms communicate and govern their data practices.

Recent evidence demonstrates that responsible data management has become a significant determinant of consumer confidence. PwC (2024) reported that data protection was the leading factor influencing consumer trust, while Cisco (2024) found that many consumers would avoid organisations they did not trust with their personal information. These findings indicate that privacy and security are no longer merely technical or compliance concerns; they shape perceived risk, willingness to disclose information, transaction completion, and the continuation of customer relationships.

Regulatory and privacy cases further demonstrate the consequences of weak governance. Actions involving Amazon's Alexa and Ring services raised concerns regarding prolonged data retention, employee access, inadequate safeguards, and the handling of deletion requests (Federal Trade Commission, 2023, 2024). Oracle's 2024 privacy settlement similarly reflected allegations concerning the creation and sale of consumer profiles without adequate authorisation, although the company denied wrongdoing (Reuters, 2024). Such cases illustrate how insufficient transparency and control may produce legal, reputational, and financial consequences. IBM (2025) also reported that data breaches continue to impose substantial organisational costs, reinforcing the strategic importance of prevention and accountable data governance.

Ethical data practices include transparent privacy communication, meaningful consent, data minimisation, secure systems, responsible personalisation, and accessible consumer control. These practices can reduce uncertainty and signal that a platform is committed to protecting consumer interests. Importantly, ethical governance extends beyond formal legal compliance. A practice may satisfy a narrow legal requirement while remaining ethically questionable when consent is confusing, data collection is excessive, algorithms manipulate consumer choices, or information is used beyond reasonable expectations. Distinguishing these concepts is therefore necessary to explain why some technically compliant practices may still fail to generate trust.

Existing e-commerce research has established the importance of usability, product quality, payment security, delivery reliability, privacy, and trust. However, less attention has been given to an integrated explanation of how ethical data practices influence loyalty through trust and how perceived privacy and security risk constrains this process. In addition, emerging technologies such as generative artificial intelligence, algorithmic recommendation systems, blockchain, and decentralised identity create new governance opportunities and risks that require ethical evaluation. This paper addresses these gaps by developing a Social Exchange Theory-based framework in which consumer trust mediates the relationship between ethical data practices and consumer loyalty, while perceived privacy and security risk moderates the relationship between ethical data practices and trust.

LITERATURE REVIEW

Evolution of E-Commerce and the Centrality of Consumer Data

E-commerce has evolved from a basic online transaction channel into a data-intensive ecosystem shaped by mobile technology, automation, artificial intelligence, and platform-based business models (Laudon & Traver, 2023). Firms now compete not only through price and product availability, but also through personalised recommendations, targeted advertising, seamless payment, rapid fulfilment, and predictive customer engagement. Consumer data therefore function as a strategic resource that supports behavioural analysis, demand forecasting, service design, and relationship management (Chen et al., 2012).

The commercial value of data must nevertheless be balanced against consumer rights and expectations. Consumers often possess limited knowledge of how their information is collected, combined, shared, or monetised (Martin & Murphy, 2017). Kishnani and Das (2024), for example, identified weaknesses in transparency, authentication, breach notification, and other security practices across e-commerce websites.

These concerns demonstrate that the continued expansion of digital commerce requires governance arrangements that protect consumers while allowing firms to use data for legitimate and beneficial purposes.

Ethical Data Practices in the Digital Marketplace

Ethical data practices refer to the responsible collection, storage, processing, sharing, and use of consumer information in ways that are transparent, secure, fair, and respectful of autonomy (Floridi & Taddeo, 2016). In e-commerce, these practices include meaningful consent, purpose limitation, data minimisation, appropriate retention periods, secure payment and information systems, responsible personalisation, understandable privacy notices, and mechanisms that allow consumers to access, correct, delete, or restrict the use of their information.

Ethical data management is particularly important because consumers must disclose information before they can fully evaluate how a platform will behave. Excessive tracking, hidden data sharing, manipulative interface design, unclear consent, or discriminatory algorithmic outcomes may provide short-term commercial benefits but can weaken trust and brand reputation over time (Martin & Murphy, 2017; Morić et al., 2024). Transparency is therefore not limited to publishing a privacy policy. It also requires firms to explain data practices in accessible language and provide consumers with choices that are understandable and practically usable. Research on algorithmic systems similarly indicates that explainability and perceived fairness can strengthen user trust and acceptance (Shin, 2021).

Ethical Data Governance Beyond Regulatory Compliance

Regulatory compliance and ethical data governance are related but conceptually distinct. Compliance refers to adherence to applicable legal requirements governing the collection, processing, retention, sharing, and protection of personal information. Regulations such as the General Data Protection Regulation establish important principles including lawfulness, transparency, purpose limitation, data minimisation, security, and accountability (European Parliament & Council of the European Union, 2016). These requirements provide an essential baseline for organisational conduct.

Ethical data governance extends beyond this minimum baseline by asking whether data practices are fair, proportionate, understandable, and respectful of consumer dignity and autonomy. A practice may be legally permissible but ethically problematic when consumers are pressured into accepting unnecessary tracking, when consent notices exploit information asymmetry, or when personalisation is designed to manipulate vulnerable users. Ethical governance therefore evaluates not only whether an organisation is allowed to use data, but also whether it should use the data in a particular manner and whether the potential benefits justify the possible harms.

This distinction strengthens the conceptual contribution of the present study. Legal compliance may reduce exposure to sanctions, but it does not automatically produce relational trust. Consumers may remain sceptical when formal compliance is not accompanied by credible transparency, meaningful control, responsible innovation, and evidence that the firm prioritises their interests. Ethical data practices are therefore positioned as relational signals of fairness and trustworthiness rather than as a simple reflection of regulatory conformity.

Data Privacy, Security, and Consumer Perceived Risk

Data privacy concerns consumers' control over personal information, whereas data security concerns the technical and organisational safeguards that prevent unauthorised access, loss, misuse, or disclosure (Smith et al., 2011). Although conceptually distinct, both influence perceived risk in online transactions. Perceived risk includes the possibility of identity theft, payment fraud, unauthorised profiling, unwanted disclosure, or other negative consequences associated with data sharing (Featherman & Pavlou, 2003).

Perceived privacy and security risk can discourage consumers from completing purchases, sharing accurate information, or maintaining relationships with a platform. Pilakaew et al. (2024) found that privacy and security risk influenced repurchase intention in online shopping, while Cisco (2024) demonstrated that consumer engagement is strongly affected by confidence in organisational data practices. Clear communication, visible security features, data minimisation, accessible controls, and prompt incident response can reduce uncertainty.

Nevertheless, consumers may continue to perceive high risk when a platform has experienced breaches, relies on opaque tracking, or operates in an environment with weak institutional protections.

Consumer Trust and Loyalty in E-Commerce

Consumer trust refers to the belief that an e-commerce platform is competent, reliable, honest, and willing to protect consumer interests (Gefen et al., 2003). Trust is especially important in virtual exchanges because consumers cannot fully observe the seller, inspect data-processing activities, or predict how information will be used after disclosure. Privacy protection and perceived security therefore operate alongside service quality and website performance as important antecedents of online trust. A meta-analysis by Kim and Peterson (2017) confirmed significant relationships among online trust, privacy perceptions, loyalty, and repeat purchase intention.

Consumer loyalty reflects continued purchasing, ongoing platform use, positive word-of-mouth, and resistance to switching (Oliver, 1999). In highly competitive digital markets, trusted platforms are more likely to retain consumers because trust reduces uncertainty and supports a favourable evaluation of future exchanges. Ashiq et al. (2023) found that e-trust contributes to e-satisfaction and e-loyalty, while Li et al. (2025) demonstrated that privacy concerns influence trust and purchase intention in live-streaming commerce. Ethical data practices may therefore strengthen loyalty indirectly by creating the conditions under which consumers perceive a platform as reliable and worthy of continued engagement.

Emerging Technologies and Ethical Data Governance

Generative artificial intelligence and algorithmic recommendation systems create opportunities for more responsive customer service, personalised product discovery, automated content creation, and fraud detection. However, these technologies may depend on extensive datasets and opaque processing, creating concerns regarding data provenance, unauthorised use, privacy leakage, harmful bias, manipulation, and the inability of consumers to understand automated decisions. The NIST Generative AI Profile identifies data privacy, information integrity, harmful bias, security, and value-chain transparency among the risks that organisations should govern across the AI lifecycle (National Institute of Standards and Technology, 2024).

Emerging AI governance frameworks reinforce the need for transparency, risk assessment, documentation, human oversight, and accountability. The European Union's Artificial Intelligence Act adopts a risk-based framework and includes obligations concerning transparency and the governance of certain AI systems and general-purpose AI models (European Parliament & Council of the European Union, 2024). For e-commerce firms, responsible implementation should include disclosure when automated systems influence recommendations, pricing, product visibility, or customer communication; testing for discriminatory or manipulative outcomes; and processes through which consumers can challenge significant automated decisions.

Blockchain and decentralised identity systems may also support traceability, credential verification, and greater consumer control over data disclosure. Decentralised identifiers are designed to enable verifiable digital identities without requiring exclusive dependence on a central identity provider (World Wide Web Consortium, 2022). These systems may reduce unnecessary disclosure by allowing consumers to prove selected attributes rather than sharing complete identity records. Nevertheless, distributed records can create challenges relating to correction, deletion, interoperability, security, accessibility, and consumer understanding. Their ethical value therefore depends on governance design rather than on the technology alone.

Synthesis and Research Gap

The literature indicates that ethical data practices, privacy protection, security, perceived risk, trust, and loyalty are closely related, but these relationships are often examined separately or as direct effects. Existing studies provide less explanation of the relational mechanism through which ethical data governance generates loyalty and the conditions that may weaken this process. The present study addresses this gap by positioning consumer trust as a mediator between ethical data practices and loyalty and perceived privacy and security risk as a

moderator of the ethical practices-trust relationship. It also differentiates ethical governance from legal compliance and incorporates emerging technological developments into the conceptual discussion.

Theoretical Underpinning

This conceptual paper is grounded in Social Exchange Theory (SET), which explains that relationships are maintained when parties perceive an exchange as beneficial, fair, and sufficiently predictable (Blau, 1964; Homans, 1958). E-commerce involves a reciprocal exchange in which consumers provide personal data, payment information, time, attention, and behavioural information, while firms provide product access, convenience, personalisation, efficient transactions, and customer support. Because the exchange occurs under conditions of information asymmetry, consumers must assess whether the expected benefits outweigh possible privacy, security, and financial costs.

SET is appropriate for explaining ethical data governance because the quality of the exchange depends not only on economic value but also on how each party treats the other. Ethical data practices signal that the firm acknowledges its responsibility toward consumers and does not intend to exploit their informational vulnerability. Informed consent, data minimisation, transparent communication, secure systems, fair algorithms, and meaningful consumer control reduce perceived costs and strengthen the perceived fairness of the relationship. In contrast, hidden tracking, excessive collection, weak security, and manipulative personalisation increase perceived costs and may prompt consumers to restrict disclosure or terminate the relationship (Martin & Murphy, 2017; Morić et al., 2024).

Trust functions as the principal relational mechanism in this exchange. Consumers cannot continuously monitor how their information is processed, so continued participation depends on the belief that the platform is competent, reliable, and committed to protecting their interests. Ethical data practices provide observable signals that consumers use to infer integrity and benevolence. Once trust develops, consumers become more willing to transact, repurchase, share necessary information, recommend the platform, and tolerate ordinary uncertainty associated with online commerce (Gefen et al., 2003; Kim & Peterson, 2017).

Loyalty represents the continuation of a favourable exchange relationship. Repeated experiences of transparent communication, secure transactions, and responsible data handling reinforce the expectation that future interactions will also be beneficial. Trust, therefore, explains how ethical practices translate into continued engagement rather than merely serving as another parallel predictor of loyalty. This mediation logic is consistent with SET because trust stabilises the exchange and reduces the need for consumers to reassess every transaction independently.

Perceived privacy and security risk serves as a boundary condition. Ethical statements and controls may have a strong trust-building effect when consumers believe that risks are manageable. However, the same practices may be less persuasive when consumers remain concerned about previous breaches, opaque technologies, unauthorised sharing, identity theft, or weak enforcement. In SET terms, high perceived risk increases the expected cost of participation and weakens the credibility of the benefits offered by the platform. This reasoning supports the proposed moderating role of perceived privacy and security risk.

Conceptual Framework and Proposition Development

The proposed framework integrates ethical data practices, consumer trust, consumer loyalty, and perceived privacy and security risk. Ethical data practices constitute the antecedent construct and include transparency, informed consent, data minimisation, secure systems, responsible personalisation, accountability, and consumer control. Consumer trust represents confidence in the platform's integrity, competence, reliability, and benevolence, while consumer loyalty includes repurchase intention, continued use, positive word-of-mouth, and reduced switching behaviour.

The framework proposes both a mechanism and a boundary condition. Consumer trust mediates the relationship between ethical data practices and loyalty by explaining how responsible organisational conduct becomes a durable customer relationship. Perceived privacy and security risk moderates the relationship between ethical

data practices and trust by determining how strongly consumers interpret ethical practices as credible evidence of protection.

Proposition 1: Ethical Data Practices and Consumer Trust

Ethical data practices are expected to positively influence consumer trust. Transparent communication reduces uncertainty about how information is collected and used, meaningful consent demonstrates respect for autonomy, and data minimisation limits unnecessary exposure. Secure systems, responsible personalisation, and accessible consumer controls further signal competence and accountability. These practices provide evidence that the platform is willing and able to protect consumer interests, thereby strengthening perceptions of integrity, reliability, and benevolence (Gefen et al., 2003; Shin, 2021).

P1: Ethical data practices positively influence consumer trust in e-commerce.

Proposition 2: Consumer Trust and Consumer Loyalty

Consumer trust is expected to positively influence loyalty because it reduces uncertainty and makes continued engagement less psychologically and financially costly. Consumers who believe that a platform is competent, honest, and protective of their information are more willing to repurchase, continue using the platform, recommend it to others, and resist switching. Prior research consistently links online trust with satisfaction, repeat purchase intention, and e-loyalty (Ashiq et al., 2023; Kim & Peterson, 2017).

P2: Consumer trust positively influences consumer loyalty in e-commerce.

Proposition 3: Mediating Role of Consumer Trust

Ethical data practices may not directly produce loyalty unless consumers recognise those practices as credible evidence of responsible organisational behaviour. Through transparent, secure, and fair data handling, firms reduce the perceived costs of data disclosure and increase confidence in the exchange. This confidence is expressed as trust, which then encourages continued engagement and advocacy. Trust therefore constitutes the relational pathway through which ethical data practices are converted into loyalty.

P3: Consumer trust mediates the relationship between ethical data practices and consumer loyalty in e-commerce.

Proposition 4: Moderating Role of Perceived Privacy and Security Risk

Perceived privacy and security risk is expected to weaken the positive relationship between ethical data practices and consumer trust. When risk is low, consumers are more likely to interpret privacy notices, security controls, and responsible data-use commitments as convincing signals of integrity and competence. When risk is high, consumers may remain concerned about hidden tracking, unauthorised sharing, cyberattacks, payment fraud, or data breaches even when firms communicate ethical practices. Under such conditions, the expected cost of participation remains high and the trust-building value of ethical practices is reduced (Featherman & Pavlou, 2003; Pilakaew et al., 2024).

P4: Perceived privacy and security risk weakens the positive relationship between ethical data practices and consumer trust in e-commerce.

DISCUSSION

The framework advances the discussion of responsible digital commerce by treating ethical data practices as relational signals rather than as purely technical controls or legal obligations. From a Social Exchange Theory perspective, consumers evaluate whether disclosing personal information produces a fair balance between benefits and potential costs. Ethical practices improve this balance by reducing information asymmetry, limiting unnecessary exposure, and demonstrating that the firm recognises its responsibilities toward consumers. This

interpretation explains why technical compliance alone may be insufficient when consumers perceive that data use remains intrusive, manipulative, or inconsistent with their expectations.

The distinctive contribution of the framework is its explanation of how and under what conditions ethical data practices influence loyalty. Trust provides the mechanism: responsible data practices strengthen perceptions of integrity, competence, and benevolence, which support repeat engagement and positive word-of-mouth. Perceived privacy and security risk provides the boundary condition: ethical practices have less influence on trust when consumers continue to anticipate substantial harm. This integrated approach extends studies that examine direct relationships among privacy, trust, and purchase intention by combining mediation and moderation within a single conceptual model.

The inclusion of emerging technologies also broadens the relevance of the framework. Generative AI and algorithmic personalisation can improve convenience but may simultaneously increase opacity, profiling, privacy leakage, and manipulation risk. Blockchain and decentralised identity may improve traceability or selective disclosure but can create challenges relating to permanence, interoperability, and accessibility. The effect of these technologies on trust therefore depends on how they are governed. Technology adoption should be assessed according to transparency, proportionality, consumer control, accountability, and the capacity to prevent or remedy harm.

Theoretical Implications

This paper extends Social Exchange Theory into the context of digital data governance by conceptualising personal-data disclosure as part of an ongoing reciprocal relationship. It demonstrates that the perceived fairness of the exchange depends on the governance of data as well as the functional benefits of e-commerce. Ethical practices reduce the perceived costs of participation and communicate that the firm accepts relational responsibilities that extend beyond formal contractual and legal obligations.

The framework also contributes by integrating ethical data practices, trust, loyalty, and perceived risk into a mechanism-and-boundary model. Trust explains the process through which ethical conduct becomes loyalty, while perceived privacy and security risk explains why the same organisational practices may generate different levels of trust across consumers and contexts. The explicit distinction between ethical governance and regulatory compliance further clarifies that ethical responsibility is not exhausted by legal conformity.

Practical Implications

E-commerce managers should embed ethical data governance into corporate strategy, product design, marketing, and customer relationship management. Privacy notices should be concise and understandable, consent should be freely given and specific, and data collection should be limited to legitimate purposes. Organisations should provide practical controls that allow consumers to access, correct, delete, or restrict the use of their information. These actions demonstrate respect for autonomy and may strengthen trust more effectively than legalistic disclosures alone.

IT and cybersecurity teams should support ethical commitments through encryption, access controls, secure authentication, system monitoring, incident-response plans, vendor assessment, and regular security audits. Firms using AI-driven personalisation should disclose when automated systems materially influence recommendations, pricing, product visibility, or customer communication. Algorithmic impact assessments, bias testing, data-provenance reviews, human oversight, and mechanisms for consumer challenge should be established before and after deployment. Where blockchain or decentralised identity systems are adopted, firms should ensure that consumers understand how credentials are stored, verified, corrected, revoked, and shared.

Boards and senior management should establish cross-functional data-governance oversight involving legal, compliance, marketing, information technology, cybersecurity, ethics, and consumer-protection expertise. Key performance indicators should extend beyond the absence of regulatory penalties to include complaint patterns, consent withdrawal, privacy-control usage, breach response, algorithmic incidents, and consumer trust. Policymakers should encourage interoperable standards and accountable AI governance while recognising

differences in national regulatory capacity. Consumers should also be provided with accessible information and tools that improve their ability to make informed privacy and security decisions.

Limitations and Future Research

As a conceptual study, this paper does not empirically validate the proposed relationships, and its framework should therefore be interpreted as a theoretically grounded basis for future testing rather than as evidence of causal effects. The discussion also draws on literature and cases from different institutional settings. Consumer expectations and the credibility of organisational data practices may vary according to culture, regulatory enforcement, digital literacy, platform type, and previous experience with privacy incidents.

Future research may operationalise ethical data practices through measurable dimensions such as transparency, informed consent, data minimisation, security protection, fairness, accountability, responsible personalisation, and consumer control. Consumer trust may be assessed through perceived integrity, competence, reliability, and benevolence, while loyalty may be measured using repurchase intention, continued platform use, positive word-of-mouth, and resistance to switching. Perceived privacy and security risk may include concerns regarding unauthorised sharing, identity theft, payment fraud, data breaches, profiling, and loss of control. Researchers should adapt validated scales from privacy, trust, perceived-risk, and e-loyalty literature and assess content validity through expert review and pilot testing.

The mediation and moderation relationships may be examined using covariance-based Structural Equation Modelling or PLS-SEM, depending on the research objective, model characteristics, sample size, and distributional assumptions. Multi-group analysis could compare countries, age groups, levels of digital literacy, prior breach experience, and different platform categories. Experiments could evaluate how changes in consent design, privacy explanations, AI disclosure, or security assurances affect trust, while longitudinal studies could determine whether trust persists after repeated transactions or privacy incidents. Qualitative case studies may also examine how firms translate ethical principles into governance structures and operational decisions.

CONCLUSION

Ethical data practices are essential for fostering consumer trust and loyalty in e-commerce. Drawing on Social Exchange Theory, this paper argues that consumers are more willing to maintain digital relationships when data exchanges are perceived as fair, transparent, secure, and respectful of autonomy. The proposed framework demonstrates that ethical data practices generate loyalty through the development of consumer trust, while perceived privacy and security risk determines whether those practices are interpreted as credible and sufficiently protective.

The study further establishes that ethical governance is broader than regulatory compliance. Legal conformity provides a necessary baseline, but sustainable trust requires proportionality, accountability, meaningful consumer control, and responsible technological innovation. As e-commerce firms increasingly adopt generative AI, algorithmic personalisation, blockchain, and decentralised identity systems, the governance of data will remain central to consumer confidence and long-term competitive sustainability. Empirical testing is now required to validate the proposed mediation and moderation relationships across different consumer, platform, and regulatory contexts.

Ethical Considerations

This conceptual paper does not involve human participants, animal subjects, or primary data collection. Therefore, formal ethical approval was not required.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Data Availability

No primary dataset was generated for this conceptual paper. The discussion is based on publicly available literature, reports, and cases cited in the reference list.

ACKNOWLEDGEMENT

The authors would like to express their sincere appreciation to the Accounting Research Institute (ARI), Universiti Teknologi MARA, Malaysia, as a Higher Institution Centre of Excellence (HICoE), under grant UiTM.800-3/1 DDJ.82 (012/2025) and the Ministry of Higher Education Malaysia for the funding and support provided, which contributed to the completion of this paper.

REFERENCES

1. Ashiq, R., Hussain, A., & Aslam, N. (2023). Exploring the effects of e-service quality and e-trust on consumers' e-satisfaction and e-loyalty: Insights from online shoppers in Pakistan. *Journal of Electronic Business & Digital Economics*, 3(2), 117-141.
2. 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.
3. Blau, P. M. (1964). *Exchange and power in social life*. John Wiley & Sons.
4. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, 36(4), 1165-1188.
5. Cisco. (2024). Cisco 2024 consumer privacy survey. Cisco.
6. DataReportal. (2025). Digital 2025: Global overview report. DataReportal.
7. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*, L119, 1-88.
8. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union*, 2024/1689.
9. Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451-474.
10. Federal Trade Commission. (2023). FTC and DOJ charge Amazon with violating children's privacy law by keeping kids' Alexa voice recordings forever and undermining parents' deletion requests. Federal Trade Commission.
11. Federal Trade Commission. (2024). Ring, LLC. Federal Trade Commission.
12. Ferrell, O. C., Fraedrich, J., & Ferrell, L. (2022). *Business ethics: Ethical decision making and cases* (13th ed.). Cengage Learning.
13. Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*, 374(2083), 20160360.
14. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.
15. Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology*, 63(6), 597-606.
16. IBM. (2025). Cost of a data breach report 2025. IBM.
17. Kim, Y., & Peterson, R. A. (2017). A meta-analysis of online trust relationships in e-commerce. *Journal of Interactive Marketing*, 38, 44-54.
18. Kishnani, U., & Das, S. (2024). Dual-technique privacy and security analysis for e-commerce websites through automated and manual implementation. *arXiv*. <https://arxiv.org/abs/2410.14960>
19. Laudon, K. C., & Traver, C. G. (2023). *E-commerce 2023-2024: Business, technology, society*. Pearson.
20. Li, W., Cujilema, S., Hu, L., & Xie, G. (2025). How social scene characteristics affect customers' purchase intention: The role of trust and privacy concerns in live streaming commerce. *Journal of Theoretical and Applied Electronic Commerce Research*, 20(2), 85.
21. Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45, 135-155.

22. Morić, Z., Dakić, V., Đekić, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy*, 4(3), 731-761.
23. National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.600-1>
24. Oliver, R. L. (1999). Whence consumer loyalty? *Journal of Marketing*, 63, 33-44.
25. Pilakaew, T., Thanitbenjasith, P., & Kamkankaew, P. (2024). The impact of consumer perceptions of privacy and security risks on re-purchasing intention for online shopping in Chiang Mai Province, Thailand. *International Journal of Sociologies and Anthropologies Science Reviews*, 4(6), 531-542.
26. PwC. (2024). Voice of the consumer survey 2024. PricewaterhouseCoopers.
27. Reuters. (2024). Oracle reaches \$115 million consumer privacy settlement. Reuters.
28. Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies*, 146, 102551.
29. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1016.
30. Wang, Y., Chen, X., & Zhang, J. (2024). Understanding consumers' continuous participation willingness in online pre-sale activities: A social exchange theory perspective. *Behavioral Sciences*, 14(11), 1094.
31. World Wide Web Consortium. (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation. <https://www.w3.org/TR/did-1.0/>