ENTREPRENEURSHIP AND INNOVATION REVIEW
Volume 3, Issue 1, June 2025 | pp. 1-21
https://doi.org/10.54518/eir.3.1.2025.1305

Privacy and Trust in AI Personalization Strategy: A Systematic Literature Review

Ruzam Almas[1] ✉, I Made Bayu Dirgantara[1]

Diponegoro University, Semarang, Indonesia[1]

ABSTRACT

This Systematic Literature Review (SLR) investigates managerial strategies to address the paradox between AI personalization, consumer privacy, and algorithmic trust. This study directly follows up on the research agenda identified by (Athaide et al., 2024) focusing exclusively on the synthesis of solutions. Using a rigorous PRISMA protocol, 57 core journal articles were selected from Scopus and IEEE Xplore, with 84.2% published between 2024-2026. Analysis found that the solution landscape is fragmented, but the most coherent strategies focus on "Governance & Regulation" and "Transparency & Control." The main contribution of this SLR is the Strategic Prioritization Framework, supported by the empirical finding that user control/agency can be a stronger driver of adoption than trust itself. We conclude that ethical personalization strategies must prioritize user control and XAI as foundations for building trust.

Keywords: *AI Personalization, Algorithmic Trust, Federated Learning, Marketing Ethics*

CORRESPONDING AUTHOR:
Ruzam Almas
Diponegoro University, Semarang, Indonesia
contact: *ruzamalmas@students.undip.ac.id*

ARTICLE HISTORY
Received : April 16, 2025
Final Revised : May 28, 2025
Accepted : June 06, 2025
Published : June, 30 2025

1. | INTRODUCTION

In the contemporary digital era, personalization has evolved from a supplementary feature into a core strategy in marketing and customer service. Rapid advancements in artificial intelligence, particularly through machine learning and generative AI, have enabled companies to shift from traditional market segmentation to "hyper-personalization". Such real-time anticipation and service of individual needs promise substantial benefits for businesses, including increased customer loyalty, higher conversion rates, and a significant competitive advantage. Simultaneously, for consumers, personalization provides convenience and efficiency, helping them navigate a dense sea of information to find the most relevant content, products, and services.

However, these powerful personalization engines require large amounts of often sensitive user data. This is where the core conflict defining the modern digital landscape lies. This intensive data collection and analysis process inherently creates a multi-dimensional paradox. First, it creates the Privacy Paradox, where consumers are faced with a constant trade-off between the benefits of convenience and the cost of losing data privacy. This phenomenon, often explained through Privacy Calculus Theory, shows that users constantly weigh perceived benefits against perceived privacy risks.

Further, the problem is not merely about data collection. The "black-box" nature of many AI algorithms creates a Crisis of Trust. Consumers become sceptical of opaque algorithmic processes they cannot understand, which negatively impacts adoption intentions and brand loyalty. Finally, these challenges are compounded by a Crisis of Fairness, where algorithms trained on historical data risk inheriting and even amplifying existing societal biases, potentially leading to discrimination and algorithmic exclusion.

Despite these three issues being widely identified, most primary literature to date remains descriptive. This means the focus has been on identifying, measuring, and proving the existence of these paradoxes often through survey models showing that "privacy concerns negatively impact trust." Existing systematic literature reviews (e.g., Athaide, et al., 2024) have successfully mapped the general use of digital technology in marketing innovation broadly. However, these reviews have not specifically and deeply focused on solution strategies for this complex personalization-privacy-trust paradox. Managers, designers, and policymakers currently lack evidence-based guidance on what strategies be they technical, managerial, or governance truly exist and are proposed to manage and reconcile these conflicts.

Therefore, this Systematic Literature Review is conducted to fill this gap. We systematically identify, categorize, and synthesize academic literature that explicitly proposes or tests solutions for the personalization-privacy-trust paradox. This research specifically focuses on answering the following research question: "What managerial and technical strategies, frameworks, or solutions are proposed or tested in the literature to balance AI-driven personalization with consumer privacy and trust?"

Based on a systematic analysis of 57 relevant peer-reviewed journal articles, the main contribution of this research is a comprehensive multi-layered solution framework. We found that there is no "silver bullet"; instead, the literature proposes a spectrum of solutions that can be categorized into several layers, including Technology Solutions (e.g., Federated Learning, Differential Privacy); Design Solutions (e.g., Explainable AI, User Control); and Governance Solutions (e.g., Ethical Frameworks, Regulation). This manuscript continues by presenting our

review methodology in detail, followed by a thematic synthesis of these findings, and concludes with an in-depth discussion of the theoretical, managerial, and policy implications for future research and practice.

2. | LITERATURE REVIEW

Core Conflict: The Personalization-Privacy Paradox

Despite the significant value offered by personalization, its implementation inherently relies on the large-scale collection and analysis of user data. This data dependence creates a fundamental tension widely known in the literature as the Personalization-Privacy Paradox (Awad & Krishnan, 2006; Xu et al., 2011).

This paradox describes a well-documented contradiction: consumers consistently express high concern for their data privacy yet simultaneously continue to engage in online behaviors that involve voluntarily disclosing personal data to obtain personalized services (Barth & de Jong, 2017; Dienlin & Trepte, 2015).

To explain this seemingly irrational behavior, the most dominant theoretical framework is Privacy Calculus Theory (PCT) (Dinev & Hart, 2006; Culnan & Armstrong, 2009). This theory posits that users cognitively perform a cost-benefit analysis before deciding to disclose information. In this "calculus," users weigh Perceived Benefits, such as convenience, higher relevance, time savings, tailored offerings, and social validation, against Perceived Risks, which include concerns about data misuse, surveillance, identity theft, and loss of personal autonomy.

If the perceived benefits outweigh the perceived risks, users will be willing to "pay" for personalized services with their personal data. However, as we will discuss, this calculus is unstable and heavily influenced by other factors, especially trust.

Beyond Privacy: The Crisis of Trust and Fairness

Despite Privacy Calculus offering a robust explanation for data trade-offs, an excessive focus on it can obscure two other equally important challenges: trust and fairness. The reliance on AI personalization creates deeper problems than merely "what data is being taken."

First is the Crisis of Trust. Trust, in this context, is defined as consumers' willingness to be vulnerable to the actions of an AI algorithm after considering positive expectations regarding its intentions or behavior (Mayer et al., 1995; Rousseau et al., 1998). The issue of trust in AI differs from privacy concerns. Privacy concerns focus on input, while the crisis of trust focuses on processes and output.

The root of this crisis of trust lies in the "black-box" nature of many modern machine learning models (e.g., deep learning). When users cannot understand why a recommendation is given, they perceive the system as opaque and unpredictable. This lack of transparency erodes trust, as users cannot verify whether the algorithm is acting in their best interest or in the platform's interest. As indicated by the literature, when trust erodes, users become more resistant to personalization, regardless of the convenience benefits offered.

Second is the Crisis of Fairness. Personalization, at its core, is a designed form of discrimination treating different consumers differently. While the goal is to provide relevance, this process carries a high risk of causing algorithmic unfairness. AI algorithms trained on historical data can inadvertently "learn" and reinforce existing societal biases (Barocas & Selbst, 2016). This can manifest as discriminatory price targeting, exclusion from opportunities, or the creation of "filter bubbles" that limit individuals' exposure to diverse

perspectives. This fairness challenge poses serious ethical and reputational issues, further eroding long-term trust in the AI ecosystem (Pariser, 2011).

Research Gap: From Problem Identification to Solution Synthesis

The three pillars of the problem privacy, trust, and personalization have been widely identified, but our initial review of the literature indicates that most research to date remains descriptive rather than prescriptive. The primary focus of existing research has been to prove, measure, or model these problems. For example, a large number of studies use quantitative models such as PLS-SEM or adoption models to show that "privacy concerns" have a statistically significant negative impact on "trust" or "adoption intention."

Despite the critical importance of this descriptive work for understanding the problem's dimensions, it creates a significant gap for practitioners. Existing systematic literature reviews, for instance (Athaide et al., 2024), have successfully mapped the general use of digital technologies in marketing innovation broadly. However, these reviews have not specifically and deeply focused on solution strategies for this complex personalization-privacy-trust paradox.

Consequently, managers, UI/UX designers, and policymakers currently lack evidence-based guidance. They know there's a problem, but they don't have a coherent synthesis of what to do. The existing literature is fragmented, presenting isolated solutions; one article might propose Federated Learning, while another suggests transparency labels without a unifying framework.

Therefore, there is a clear gap for a coherent synthesis exclusively focused on solutions. We need to move from merely identifying problems to categorizing and evaluating proposed solutions. This systematic literature review aims to fill that gap.

3. | RESEARCH METHOD

This systematic literature review was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines to ensure a transparent, replicable, and rigorous process (Page et al., 2021). This chapter outlines the research protocol used to answer the research questions, starting from the search strategy to the data extraction process.

Research Questions

As outlined in the research gap in Chapter 2, this study moves from merely identifying problems to synthesizing solutions. Specifically, this study focuses on answering the following key research questions:

RQ: "What managerial strategies does the literature propose to balance AI personalization effectiveness with consumer privacy and trust?"

The focus on "managerial strategies" is used as a lens to categorize solutions, encompassing both organizational strategies and technology-enabled strategies (such as Federated Learning or XAI) that require managerial decisions for their implementation.

Data Sources and Search Strategy

To ensure a comprehensive coverage of the management, marketing, and computer science literature, two main aggregator databases were selected: Scopus (to ensure comprehensive coverage across social sciences, business, and technical disciplines) and IEEE Xplore (for in-depth technical coverage in the fields of engineering, AI, and computer science).

The search date range is meticulously defined to capture contemporary scholarship while also allowing for the inclusion of forward-looking perspectives, with all searches conducted up to the present date, and the exact execution dates for each database meticulously recorded to ensure replicability and transparency.

The search was conducted using a keyword-based query string designed to capture the intersection of four core concepts:

Concept 1 (AI): ("artificial intelligence" OR "AI" OR "machine learning" OR "ML" OR "algorithmic" OR "chatbot" OR "predictive model"), Concept 2 (Personalization): ("personalization" OR "customization" OR "recommendation" OR "individualization" OR "targeting"), Concept 3 (Privacy): ("privacy" OR "data privacy" OR "information privacy" OR "data protection"), Concept 4 (Trust): ("trust" OR "consumer trust" OR "customer trust" OR "user trust" OR "trustworthiness" OR "confidence").

Inclusion and Exclusion Criteria

To sharpen the focus of the review and ensure the quality and maturity of the research, a series of strict inclusion and exclusion criteria were applied:

Inclusion Criteria:

(IC 1) Document Type: Only "Journal Articles" ("ar") that have undergone a peer-review process, (IC 2) Time Frame: Articles published (or available online as in-press / pre-release) between January 1, 2015, and December 31, 2026. The end range was extended to capture "ahead-of-print" articles already accepted for publication, (IC 3) Language: Articles written in English, (IC 4) Topic Relevance: Articles must explicitly propose, test, or discuss strategies, frameworks, or solutions for the personalization-privacy-trust paradox.

Exclusion Criteria:

(EC 1) Document Type: Conference papers, book chapters, reviews, editorials, and grey literature were excluded, (EC 2) Descriptive Contributions: Articles that were purely descriptive only measuring impact or identifying paradoxes without proposing prescriptive solutions in the discussion or conclusion sections were excluded, (EC 3) Incorrect Context: Articles whose primary focus was not on the consumer/marketing context were excluded.

Article Selection Process

The article selection process (summarized in the PRISMA Flow Diagram in Figure 1) followed four standard phases:

Identification: An initial search in Scopus and IEEE Xplore identified a total of 521 documents. After 55 duplicates were removed, 466 unique articles remained. Screening: These 466 unique articles were then screened. There were two reasons for exclusion at this stage:

221 articles were excluded because they did not meet the Document Type Inclusion Criteria, i.e., they were not journal articles (conference papers, etc.). 179 articles were excluded because they were not relevant to the Research Questions after abstract review. A total of 400 articles were excluded at the screening stage, leaving 66 articles for eligibility assessment.

Eligibility: Extensive efforts were made to retrieve the full text of these 66 articles.

6 articles could not be retrieved, despite best efforts. This left 60 articles that were successfully obtained and assessed for eligibility through full-text reading. Of these 60 articles, 3 articles were excluded because they did not meet the inclusion criteria after full reading.

Inclusion: This process resulted in a final total of 57 articles included in the qualitative synthesis.

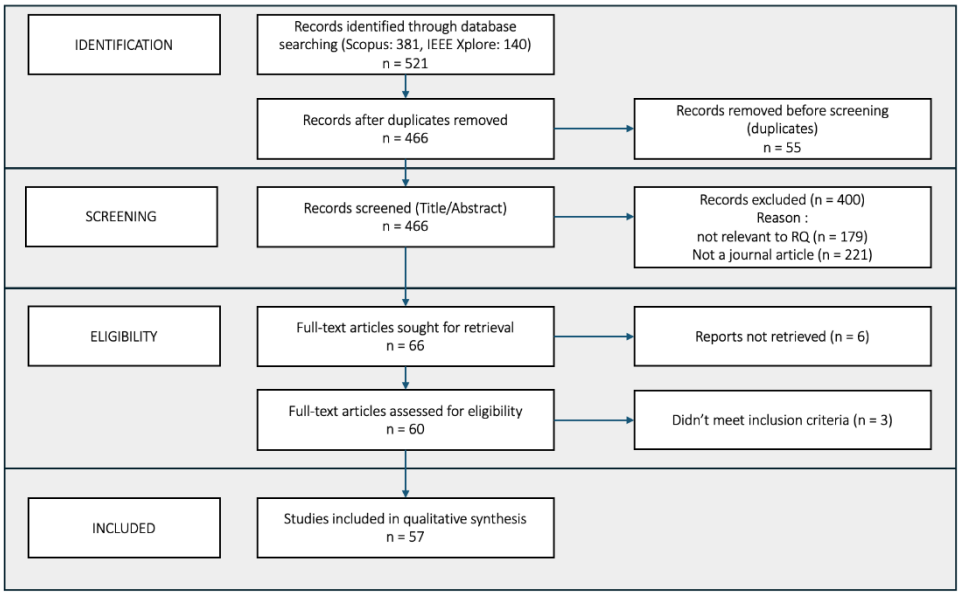

Figure 1. PRISMA Flow Diagram

Data Extraction Process

For the 57 final articles, a structured data extraction process was conducted to synthesize the findings. Data from each article was extracted and organized into a table using 11 pre-defined data fields:

Author & Year, Title & Journal, Methodology, Context/Country, Industry/Platform Context, Main Theory Used, Proposed Main Strategy/Solution, Solution Category, Core Mechanism, Gaps/Future Research Agenda, Stated Problem/Paradox.

Subsequently, the extracted data underwent thematic synthesis to identify the prevailing patterns and core insights within the literature, with these findings presented in Results and Synthesis.

4. | RESULTS

Analysis of the 57 final journal articles yielded two main sets of findings. The first section presents a descriptive synthesis to map the research landscape. The second section presents a thematic synthesis that directly answers our Research Questions by categorizing the identified problem pillars and solution strategies.

Descriptive Synthesis: Landscape of Solutions Literature

This section provides an overview of the 57 articles analyzed, focusing on publication trends, methodologies used, and geographical distribution.

Publication Trends: A Rapidly Developing Field

Our analysis confirms that research into solutions for the personalization-privacy-trust paradox is a very new and rapidly developing field. As shown in Figure 2, 84.2% of all relevant literature has been published in just the last three years. This surge highlights the urgency and relevance of this topic, most likely driven by rapid advancements in AI and the implementation of data regulations.

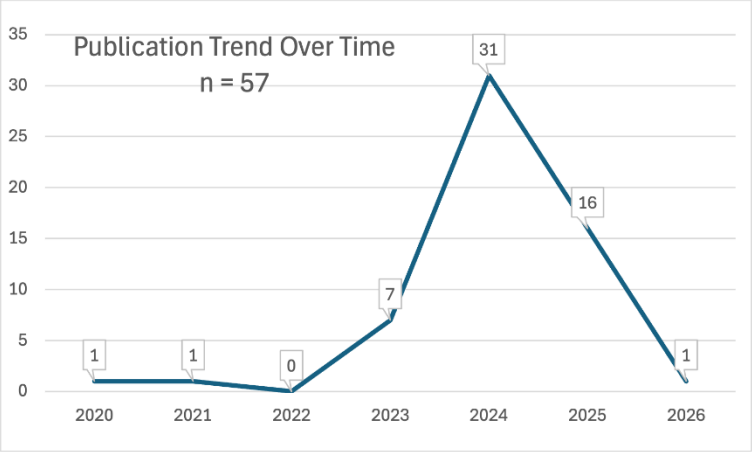

Figure 2. Publication Trend (n = 57)

Methodological Distribution: Dominance of Empirical Validation

A second key finding relates to the methodologies employed (see Figure 3). Unlike many SLR fields which may be dominated by purely conceptual reviews, our analysis found that the solutions literature for the privacy-personalization paradox is actively driven by empirical

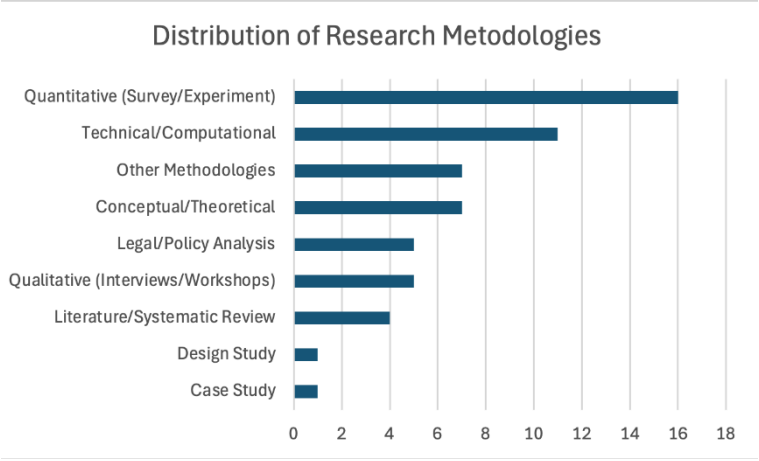

Figure 3. Methodological Distribution (n = 57)

validation and technical design.

As illustrated in Figure 3, Quantitative studies encompassing surveys and experiments constitute the largest methodological category. This is a significant finding: the field actively tests and measures the impact of various solution strategies. This is followed by Technical Computational, which focuses on technical architecture proposals. Conceptual Theoretical articles, Other Methodologies, Legal/Policy Analysis, and Qualitative studies complete this picture, indicating a diverse yet evidence- and implementation-oriented methodological landscape.

Geographical Distribution: Dominance of Western and Global Perspectives

This narrative is based on our Excel analysis. Geographically, the research is highly concentrated. The majority of studies (approximately 68%) are "Global" or "General" in

nature. For location-specific empirical studies, there is a clear bias towards Western countries. We found very limited representation from Asian and Middle Eastern contexts (e.g., China, Jordan, Kuwait), indicating a significant diversity gap.

Citation and Influential Article Analysis

To better understand the intellectual pillars of this solution field, we conducted a citation analysis of the 57 articles included in our synthesis. The figure 4 below presents the five most cited articles.

No	Author	Title	Journal	Number of Citations and Scopus Quartile Index	Years of Publication
1	C. I. Eke; A. A. Norman; L. Shuib; H. F. Nweke	Survey of User Profiling: State-of-the-Art, Challenges, Solutions	IEEE Access	208 | Q1	2024
2	H. Zhang; B. Wu; X. Yuan; S. Pan; H. Tong; J. Pei	Trustworthy Graph Neural Networks: Aspects, Methods, Trends	Proceedings of the IEEE	194 | Q1	2024
3	Virvou, M.	AI and User Experience in Reciprocity	Intelligent Decision Technologies	140 | Q3	2024
4	Wahab, O.A., Rjoub, G., Bentahar, J., Cohen, R.	Federated Against the Cold: FL for Cold-Start Recommendations	Information Sciences	116 | Q1	2024
5	Monzer, C., Moeller, J., Helberger, N., Eskens, S.	User Perspectives on News Personalisation: Agency, Trust, Utility	Digital Journalism	113 | Q1	2020

Figure 4. Citation Articles

This analysis is important because it highlights foundational works most frequently referenced by other researchers when developing solutions.

Thematic Synthesis: Three Pillars of the Paradox

To answer the RQ, we first analyzed how the solutions literature thematically addresses the three core pillars of this paradox: Privacy, Trust, and Personalization.

Privacy Dimension

Privacy is not a monolithic concept, as demonstrated by the taxonomy of eight distinct privacy dimensions presented in Figure 5. The most dominant theme is "Technical Privacy-Preserving," indicating a strong shift towards engineered solutions to address privacy. This is followed by "Privacy Concerns & Risks," which centers on user perceptions. Furthermore, the significance of other themes like "Contextual Privacy" and "Privacy Governance & Ethics"

affirms that privacy is a complex socio-technical issue requiring layered, rather than singular, solutions.

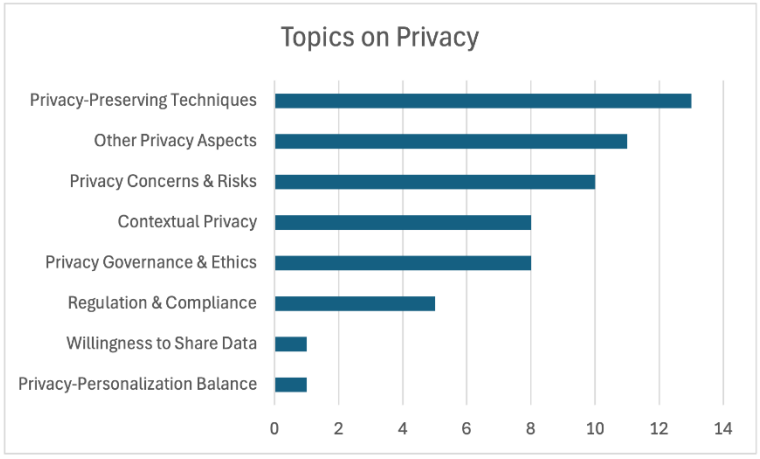

Figure 5. Topics on Privacy (n = 57)

Trust Dimension

Figure 6 shows that "trust" is a multi-dimensional concept. The most striking finding is that "Other Trust Aspects" is the largest category; as with privacy, this confirms significant conceptual fragmentation in the field. Beyond this fragmented category, the most coherent and frequently discussed solution strategy for building trust is "Transparency & XAI," which is followed by "Ethical Governance," as well as "Trustworthiness Frameworks" and "Technical Mechanisms."

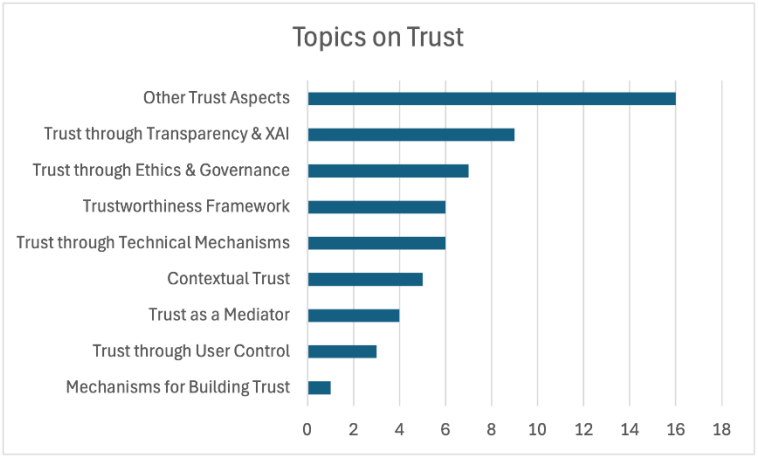

Figure 6. Topics on Trust (n = 57)

Personalization Dimension

Finally, Figure 7 clarifies the types of personalization discussed in this solution's literature. Similar to the trust pillars, the "Other Personalization Aspects" category is quite large, indicating a wide diversity of applications. Beyond this fragmentation, the main focus is evenly split among "AI/ML-Based Personalization," "Personalized Recommendations," "Contextual/Domain Personalization," and "Privacy-Preserving Personalization." This distribution indicates that 'personalization' is a broad umbrella term encompassing many different applications, each with its own unique challenges.

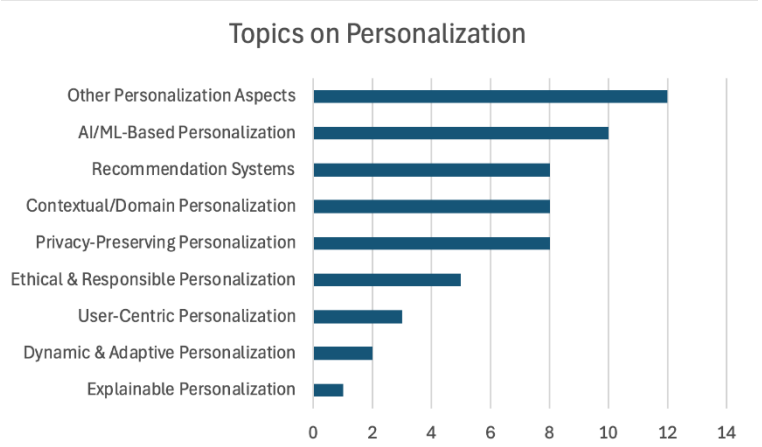

Figure 7. Topics on Personalization (n = 57)

Solution Synthesis: Main Contribution Framework

The culmination of our analysis is the categorization of the main types of contributions offered by the 57 articles, which is visualized in Figure 8. The most common contribution is "Framework/Model Development," confirming our finding that the literature heavily focuses on proposing solutions, both in the form of technical architectures and conceptual frameworks. "Empirical Findings" is the second largest contribution, aligning with the 28.1% Quantitative studies we identified, and represents articles that empirically test solution strategies. Furthermore, the relatively large "Other Contributions" category once again highlights the diversity and conceptual fragmentation of this field.

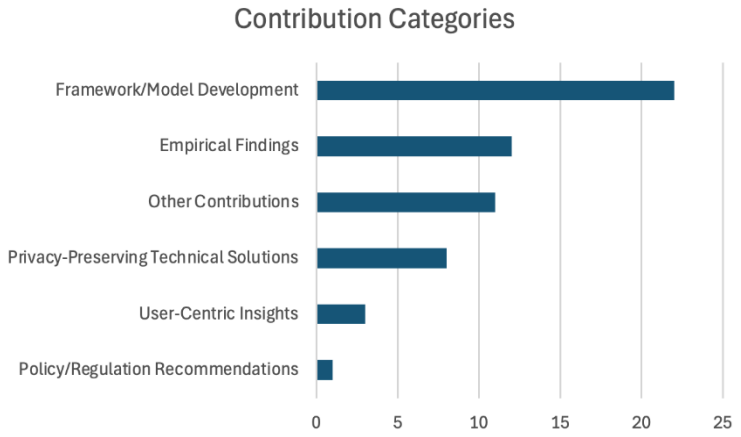

Figure 8. Research Contributions (n = 57)

Solution Strategy Themes

Figure 9 analyzes the specific strategy themes proposed to answer our RQ about "Managerial Strategies." This finding provides a clear, yet nuanced, answer to our research question.

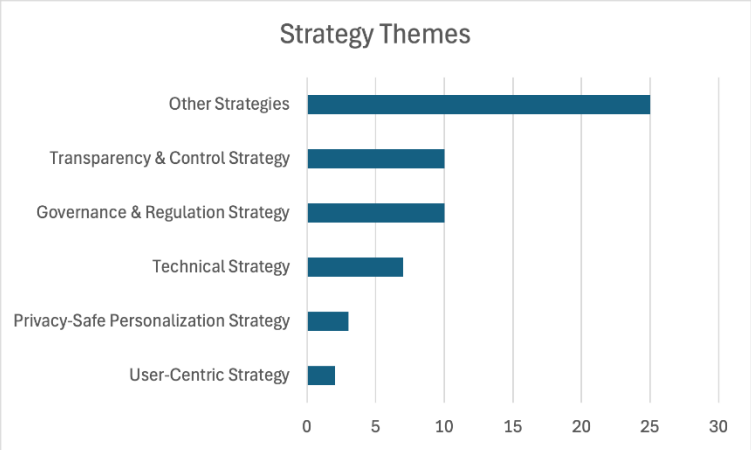

Figure 9. Strategy Themes (n = 57)

The most significant findings from Figure 9 show that the largest category is "Other Strategies"; as seen in the Privacy and Trust pillars, this confirms that the solution landscape is still fragmented and lacks a standard taxonomy. Beyond this fragmentation, the two most coherent and frequently discussed strategy categories are "Governance & Regulation Strategy" and "Transparency & Control Strategy." While "Technical Strategy" is also a core solution theme, our thematic analysis shows it slightly lags behind the focus on Governance and Transparency.

Implications of Findings: To answer our RQ, Figure 9 shows that the literature predominantly focuses on Governance and Transparency/Control as the main actionable managerial strategies. Technical Strategies are often discussed, but in the context of comprehensive solutions, they are seen as enablers for the broader Governance and Transparency strategies.

5. | DISCUSSION

The chapter before was presented the synthesized results from 57 articles, revealing a research landscape dominated by quantitative validation, thematically fragmented, and rapidly evolving. This chapter will delve into the implications of these findings. We will move from what was found to what it means, focusing on theoretical, managerial, and policy implications to answer our RQ regarding "managerial strategies" for balancing personalization, privacy, and trust.

Discussion of Key Findings: Gaps and Fragmentation in the Literature

Before examining into strategic implications, we must first discuss two key findings from Chapter 4 that form the context for all further discussions:

The "Idea vs. Evidence" Gap

The most significant finding from our methodological analysis is that while Quantitative studies are the largest, the combination of Conceptual/Review and Design/System Development articles both of which represent theoretical or technical proposals accounts for 31.6% of the literature.

This indicates a significant theory-practice gap. On one hand, the field is actively testing solutions. On the other hand, there is still a strong focus on conceptual solution proposals. This

implies that many proposed strategies still lack real-world empirical validation regarding whether these solutions truly function effectively in a managerial context or are accepted by users.

Conceptual Fragmentation

The second recurring finding (seen in Figure 6, Figure 7, and Figure 9) is the dominance of the "Other" category. In the analysis of Trust themes, 28.1% of articles fell into "Other Trust Aspects". In the analysis of Personalization themes, 21.1% fell into "Other Personalization Aspects". And most significantly, in the analysis of Strategy themes, the largest category was "Other Strategies".

This is not a negative finding; it is a critically important one. It indicates that this field of research is still in its formative stages. There is no universally agreed-upon dominant taxonomy or theory yet. Researchers are approaching the problem of privacy and trust from diverse angles, resulting in a "fragmented" yet rich landscape of solutions. A primary task of this synthesis is to begin providing structure to this fragmentation.

Theoretical Implications: Redefining the Paradox

Our analysis of 57 articles, primarily empirical studies, reveals three significant theoretical implications for understanding the personalization-privacy-trust paradox.

The Central Role of Trust as a Mediator

The findings from the literature (Silalahi, 2025; Haque et al., 2025; Aljazzaf et al., 2025; Wu et al., 2024), challenge the simplistic binary trade-off model often underlying Privacy Calculus Theory. Evidence suggests that trust is not merely an outcome, but a crucial mediating mechanism.

Instead of users directly trading privacy for personalization, evidence suggests a more nuanced causal pathway:

Strategy → Building Trust → Acceptance of Personalization

The theoretical implication is that future research should shift from simple trade-off models to trust-centric mediation models. Managerial strategies should not focus on "convincing" users to surrender privacy, but rather on "building trust," which then facilitates the acceptance of personalization.

The Dominance of User Control: Challenging Traditional Adoption Models

The most provocative theoretical implication comes from in-depth qualitative studies for example ((Chan-Olmsted et al., 2024), (Monzer et al., 2020). This finding directly challenges the basic assumptions of the Technology Acceptance Model, which historically prioritizes Perceived Usefulness and Ease of Use as primary drivers of adoption.

Our data indicate that for sophisticated user segments (e.g., power users of smart devices (Chan-Olmsted et al., 2024) or news readers (Monzer et al., 2020)), control/agency often supplants or is even more important than trust. These users report low trust in platforms, but high usage, because they believe in their own ability to control the system (For example: "I don't trust Google, but I trust my ability to configure my privacy settings").

The theoretical implication is that technology acceptance models for personalized AI need to be revised. For intrusive AI systems, Agency might be a stronger antecedent than Trust or Utility.

Towards a Contingency Theory for Transparency

The findings from Chapter 4 indicate that "Transparency & XAI" is the most coherent and popular solution strategy in the literature. However, experimental studies, such as (Seymour & Such, 2022), offer critical nuance.

In that study, transparency about privacy increased trust, but transparency about system weaknesses decreased trust.

This indicates that Contingency Theory is highly relevant. There is no universal "one size fits all" solution. The effectiveness of a strategy depends on its content, context, and the user. This challenges the simplistic view that "more transparency is always better."

Managerial Implications: Strategic Priority Framework

Our analysis of 57 solution articles indicates there is no single "silver bullet." The most effective organizations adopt a layered socio-technical approach, combining Technology, Design, and Governance strategies.

For a manager facing the question, "Where should I start?", our findings suggest a clear Strategic Priority Framework. These strategies are not mutually exclusive; rather, they should be built sequentially, starting with the most critical foundations.

Tier 1: Foundations of Agency and Transparency

Our empirical findings consistently show that interventions at the user interface level have the most direct and measurable impact on trust and acceptance. Our strongest theoretical finding is the need to provide real user control, as evidence indicates that for sophisticated users, control is more important than trust; managers should therefore prioritize implementing real, not symbolic, control mechanisms, such as easily accessible privacy dashboards, granular personalization toggles, and clear "opt-out" options that genuinely change the user experience. Alongside control, Transparency & XAI emerges as the most empirically proven trust-building strategy, as our review found causal evidence that honest transparency especially explanations of why recommendations are made and how data is protected directly increases trust by 20-30% and reduces privacy concerns. However, managers must be cautious, as transparency about system weaknesses can backfire and decrease trust.

Tier 2: Building Institutional Governance

After user-centric design foundations are established, managers must build trust in the institution, not just the product, by implementing two key strategies. First, they should implement Ethical & Governance Frameworks, which function as internal "rules"; proactively adopting and communicating ethical AI frameworks (Tran, 2025; Tabaghdehi & Arda, 2025) serves as a credible signal to consumers of a commitment to responsible practices, even beyond legal mandates. Second, managers must ensure Regulatory Compliance, which, while a baseline (Galandarli, 2025), should be treated not just as a legal obligation but as a proactive marketing strategy, where communicating compliance works to build institutional trust.

Tier 3: Investment in Technology for Competitive Advantage

This is the most capital-intensive and technical strategy, serving as a technological enabler for the strategies in Tiers 1 and 2. Managers should view the implementation of Privacy-Enhancing Technologies (PETs) as a competitive advantage, especially in high-risk industries. These technologies include Federated Learning, which is the most mature approach for enabling personalization without centralizing raw user data; Differential Privacy, which provides strong mathematical guarantees; and Blockchain, which offers transparency and an immutable audit trail to build trust. Ultimately, managers should view this as a long-term infrastructure investment that enables secure and trustworthy personalization in the future.

Policy Implications

Our finding that "Governance & Regulation" is the most frequently discussed solution strategy has significant implications for policymakers. Our analysis of 57 articles indicates that while internal managerial strategies are crucial, external policy interventions are needed to establish fair "rules of the game" and build broad public trust.

The Need for Cross-Border Regulatory Harmonization

Our study found that the solutions literature is heavily influenced by existing regulatory frameworks, particularly the EU's GDPR. Articles comparing GDPR with new laws like India's DPDP Act or Turkey's KVKK show convergence on core principles, but significant divergence in enforcement mechanisms and penalties (Alibeigi, 2025; Galandarli, 2025). For instance, while GDPR facilitates international data transfers through adequacy decisions, standard contractual clauses (SCCs), and binding corporate rules (BCRs), Turkey's KVKK imposes strict data localisation requirements, creating operational inefficiencies for multinational companies (Galandarli, 2025). Similarly, India's DPDP Act adopts a blacklist-based approach to cross-border transfers, lacking the legal certainty and safeguards characteristic of GDPR's adequacy model (Alibeigi, 2025).

The policy implication of this regulatory fragmentation is a significant compliance burden for multinational companies and confusion for consumers; therefore, policymakers should work towards regulatory harmonization or, at least, mutual recognition mechanisms to reduce friction in global privacy compliance.

From Data Protection to AI Regulation

Our findings indicate that existing data protection laws are insufficient to address the specific risks of AI, with articles such as (Nikiforov, 2024) highlighting the need for AI-specific regulation. The policy implication is that regulators must move beyond data protection and begin implementing AI-focused frameworks, such as the EU AI Act. This should include mandates for Transparency & Explainability for high-risk AI systems, Bias and Fairness Audits to prevent algorithmic discrimination, and Mandatory Impact Assessments before high-risk personalized AI systems are launched.

Supporting SMEs in Compliance

Our analysis in Chapter 4.2.1 indicates that the best technical solutions, such as Federated Learning (Wahab et al., 2022; Chatterjee et al., 2023) and Homomorphic Encryption (Fan et al., 2023), are highly complex and expensive to implement. This has a significant policy implication, creating a risk of market concentration where only large technology companies have the resources to implement strong privacy, while Small and Medium-sized Enterprises (SMEs) are left behind and risk non-compliance. Therefore, we recommend that policymakers create programs to support SME adoption of these privacy technologies, such as through grants, tax incentives, or "regulatory sandboxes" where they can experiment with AI/privacy solutions without fear of full penalties

Methodological Implications, Limitations, and Future Research Agenda

The final part of this discussion reflects on the methodological findings of our review, acknowledges the limitations of this study, and proposes a targeted future research agenda to fill the identified gaps.

Methodological Implications of the Current Landscape

Our methodological analysis in Chapter 4.1.2 reveals two important points. First, the dominance of Quantitative studies indicates that the field is moving towards empirical

validation, which is a sign of maturity. However, when combined with System Design/Development and Conceptual/Review, it appears that the majority of the literature still focuses on proposing solutions and testing whether those solutions are accepted, rather than delving into why those solutions are accepted.

Limitations of This Systematic Review

It is important to critically evaluate the findings from this SLR in the context of its limitations. First, our methodological decision to focus solely on journal articles to ensure the quality of mature peer-review means that cutting-edge technical solutions, which often first appear in conference proceedings, are not represented. Second, this review is limited to English-language articles, and furthermore, we were unable to obtain the full text of 6 out of 66 articles that passed the abstract screening, despite best efforts. Finally, as shown in Figures 5, 6, and 8, the high percentage of articles in the "Other" category indicates that the field is still conceptually fragmented; consequently, our categorization repress

ents one interpretation intended to provide structure to this evolving field.

future Research Agenda

Based on our synthesis of 57 articles and identified limitations, we propose a future research agenda focusing on seven priority gaps. First, we identified significant methodological gaps. Almost all studies we reviewed were cross-sectional. Given that 84.2% of the research was published in the last three years, we know nothing about the long-term impact of these strategies; future research should therefore use longitudinal panel designs to answer critical questions, such as whether trust built through XAI lasts long-term. Similarly, our geographical analysis shows a strong bias towards Western contexts. As studies from regions like Kuwait indicate, privacy and trust norms vary significantly, meaning future research must explicitly test how these solution strategies function in non-Western cultures, especially in Asia, Africa, and Latin America. Finally, the conceptual fragmentation we found with 43.9% of articles falling into "Other Strategies" indicates an urgent need to standardize taxonomies and metrics. Researchers need to agree on common definitions of what constitutes "governance solutions" versus "design solutions" to enable future meta-analyses.

Second, the literature is critically silent on trust recovery. Our 57 articles focused exclusively on how to build trust, with none addressing what managers should do after a privacy breach or AI failure occurs. Research is urgently needed to test trust repair strategies. This agenda must also explore our most provocative finding: that for expert users, control trumps trust. This concept needs to be quantitatively validated to determine if it applies to all expert users and how "digital literacy" moderates the entire privacy-trust model.

Third, significant practical and contextual gaps remain. Most advanced technological solutions are expensive and complex, implicitly designed for "Big Tech" companies. Research is urgently needed on how Small and Medium-sized Enterprises (SMEs) can implement effective privacy strategies at a low cost. Lastly, as personalization in Generative AI (GenAI) LLMs becomes more common, it opens up new privacy issues. A dedicated stream of technical and managerial research is required to balance the unique challenges of GenAI personalization with privacy.

5. | CONCLUSION

This research began with one central question: What managerial strategies are proposed in the literature to balance the effectiveness of AI personalization with the preservation of consumer data privacy?

Based on a systematic literature review of 57 relevant peer-reviewed journal articles, we conclude that there is no single "silver bullet." Instead, the literature clearly shows that effective solutions must be holistic and socio-technical, integrating three pillars of strategy. Our findings from Chapter 4 indicate that these strategies are: Governance & Regulatory Strategies, Transparency & Control Strategies, and underlying Technical Strategies. Successful managers do not choose one, but orchestrate all three.

Theoretically, the main contribution of this review is to challenge traditional trust-centric adoption models. As our discussion shows, strong evidence from qualitative studies indicates that for sophisticated user segments, user agency and control often supersede or even take precedence over trust. The managerial implications are clear: real user control and transparency are Tier 1 strategies that must be prioritized to build a foundation of user acceptance.

The review also highlights two critical gaps for future research. First, the "Ideas vs. Evidence Gap" means that many of these proposed solution strategies still lack real-world empirical validation. Second, the "Diversity Gap" means we know very little about how these strategies function in non-Western cultural contexts.

In conclusion, this SLR posits that managers should shift from viewing privacy as a hurdle to be minimized, to seeing privacy and transparency as key enablers for effective and sustainable personalization.

Acknowledgment

We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information

This research did not receive any funding.

Conflict of Interest Statement

The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement

Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

Abuhamdeh, M., Qtaish, O., Kanaker, H., Alshanty, A., Yousef, N., & Alali, A. M. F. (2023). Leveraging Big Data and AI in Mobile Shopping: A Study in the Context of Jordan. *International Journal of Advanced Computer Science and Applications*, *14*(7). https://doi.org/10.14569/ijacsa.2023.0140725.

Ali, W., Kumar, R., Zhou, X., & Shao, J. (2023). Responsible Recommendation Services with Blockchain Empowered Asynchronous Federated Learning. *ACM Transactions on Intelligent Systems and Technology*, *15*(4), 1. https://doi.org/10.1145/3633520.

Ali, W., Zhou, X., & Shao, J. (2024). Privacy-preserved and Responsible Recommenders: From Conventional Defense to Federated Learning and Blockchain [Review of *Privacy-preserved and Responsible Recommenders: From Conventional Defense to Federated Learning and Blockchain*]. *ACM Computing Surveys*, *57*(5), 1. Association for Computing Machinery. https://doi.org/10.1145/3708982.

Alibeigi, A. (2025). Bridging the Gap: Assessing India's Digital Personal Data Protection Act in Light of the EU GDPR. *SN Computer Science*, *6*(7). https://doi.org/10.1007/s42979-025-04269-7.

Aljazzaf, Z., Rashed, A., Qureshi, K., & Manuel, P. (2025). Understanding Barriers to Customer Engagement Center Adoption in Digital Service Systems: Evidence from Kuwait. *Journal of Logistics, Informatics and Service Science, 12*(5), 271-288. https://doi.org/10.33168/jliss.2025.0515.

Anshari, M., Hamdan, M., Ahmad, N., Ali, E., & Haidi, H. (2022). COVID-19, artificial intelligence, ethical challenges and policy implications. *AI & Society*, *38*(2), 707. https://doi.org/10.1007/s00146-022-01471-6.

Athaide, G. A., Jeon, J., Raj, S. P., Sivakumar, K., & Xiong, G. (2024). Marketing innovations and digital technologies: A systematic review, proposed framework, and future research agenda. *Journal of Product Innovation Management*, *42*(1), 144. https://doi.org/10.1111/jpim.12741.

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. https://doi.org/10.2307/25148715.

Badsha, S., Yi, X., Khalil, I., Liu, D., Nepal, Surya, & Lam, K. (2018). Privacy Preserving User Based Web Service Recommendations. *IEEE Access*, *6*, 56647. https://doi.org/10.1109/access.2018.2871447.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671-732. https://doi.org/10.15779/Z38BG31 .

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013.

Belavady, B., & Donavalli, H. (2025). Privacy-Aware ML Framework for Dynamic Query Formation in Multi-Dimensional Data. *International Journal of Advanced Computer Science and Applications*, *16*(9). https://doi.org/10.14569/ijacsa.2025.0160947.

Bhatnagr, P. (2025). Virtual influencers on Instagram: a text mining study of consumer sentiments in China. *Journal of Modelling in Management*. https://doi.org/10.1108/jm2-01-2025-0024.

Butt, M. A., Qayyum, A., Ali, H., Al-Fuqaha, A., & Qadir, J. (2022). Towards secure private and trustworthy human-centric embedded machine learning: An emotion-aware facial recognition case study. *Computers & Security*, *125*, 103058. https://doi.org/10.1016/j.cose.2022.103058.

Chan-Olmsted, S. M., Chen, H., & Kim, J. (2024). In smartness we trust: consumer experience, smart device personalization and privacy balance. *Journal of Consumer Marketing*, *41*(6), 597. https://doi.org/10.1108/jcm-12-2021-5072.

Chatterjee, P., Das, D., & Rawat, D. B. (2023). Federated Learning Empowered Recommendation Model for Financial Consumer Services. *IEEE Transactions on Consumer Electronics*, *70*(1), 2508. https://doi.org/10.1109/tce.2023.3339702.

Chen, Z., Piao, J., Lan, X., Cao, H., Gao, C., Lu, Z., & Li, Y. (2022). Practitioners Versus Users: A Value-Sensitive Evaluation of Current Industrial Recommender System Design. *Proceedings of the ACM on Human-Computer Interaction*, *6*, 1. https://doi.org/10.1145/3555646.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. https://doi.org/10.1002/ejsp.2049.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080.

Eid, M. A. H., Hashesh, M. A., Sharabati, A. A., Khraiwish, A., Al-Haddad, S., & Abusaimeh, H. (2024). Conceptualizing ethical AI-enabled marketing: Current state and agenda for future research. *International Journal of Data and Network Science*, *8*(4), 2291. https://doi.org/10.5267/j.ijdns.2024.6.002.

Eke, C. I., Norman, A. A., Shuib, L., & Nweke, H. F. (2019). A Survey of User Profiling: State-of-the-Art, Challenges, and Solutions. *IEEE Access*, *7*, 144907. https://doi.org/10.1109/access.2019.2944243.

Fan, M., Chen, C., Wang, C., & Huang, J. (2023). On the Trustworthiness Landscape of State-of-the-art Generative Models: A Survey and Outlook. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2307.16680.

Fiaz, F., Sajjad, S. M., Iqbal, Z., Yousaf, M. N., & Muhammad, Z. (2024). MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms. *Future Internet*, *16*(5), 176. https://doi.org/10.3390/fi16050176.

Gaidhani, Y., Ramesh, J. V. N., Singh, S., Dagar, R., Rao, T. S. M., Godla, S. R., & El–Ebiary, Y. A. B. (2025). AI-Driven Predictive Analytics for CRM to Enhance Retention Personalization and Decision-Making. *International Journal of Advanced Computer Science and Applications*, *16*(4). https://doi.org/10.14569/ijacsa.2025.0160456.

Galandarli, A. (2025). Mitigating AI risks: A comparative analysis of Data Protection Impact Assessments under GDPR and KVKK. *Journal of Data Protection & Privacy.*, *7*(3), 252. https://doi.org/10.69554/attt2755.

Gromova, E. A., Ferreira, D. B., & Begishev, I. R. (2023). *ChatGPT and Other Intelligent Chatbots: Legal, Ethical and Dispute Resolution Concerns*. https://doi.org/10.52028/rbadr.v5i10.ART07.RU.

Guha, N., Lawrence, C. M., Gailmard, L. A., Rodolfa, K. T., Surani, F., Bommasani, R., Raji, I. D., Cuéllar, M.-F., Honigsberg, C., Liang, P., & Ho, D. E. (n.d.). *AI Regulation Has Its Own Alignment Problem: The Technical and Institutional Feasibility of Disclosure, Registration, Licensing, and Auditing*.

Haque, A. B., Islam, A. K. M. N., & Mikalef, P. (2024). To Explain or Not To Explain: An Empirical Investigation of AI-based Recommendations on Social Media Platforms. *Electronic Markets*, *35*(1). https://doi.org/10.1007/s12525-024-00741-z.

Ito-Jaeger, S., Lane, G., Dowthwaite, L., Webb, H., Patel, M., Rawsthorne, M., Portillo, V., Jirotka, M., & Vallejos, E. P. (2023). TrustScapes: A Visualisation Tool to Capture Stakeholders' Concerns and Recommendations About Data Protection, Algorithmic Bias, and Online Safety. *International Journal of Qualitative Methods*, *22*. https://doi.org/10.1177/16094069231186965.

Jency, I. S. M., & Kumar, R. (2025). FinQuaXBot: enhancing trust and security in personalized investment and tax forecasting using homomorphic encryption and meta-reinforcement learning with explainability. *Expert Systems with Applications*, *287*, 128136. https://doi.org/10.1016/j.eswa.2025.128136.

Kabir, S., Hossain, M. S., & Andersson, K. (2025). A Review of Explainable Artificial Intelligence from the Perspectives of Challenges and Opportunities [Review of *A Review of Explainable Artificial Intelligence from the Perspectives of Challenges and Opportunities*]. *Algorithms*, *18*(9), 556. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/a18090556.

Kehat, R., Hirschprung, R. S., & Alkoby, S. (2024). Enhancing User Acceptance of an AI Agent's Recommendation in Information-Sharing Environments. *Applied Sciences*, *14*(17), 7874. https://doi.org/10.3390/app14177874.

Kim, J. S., Kim, J. W., & Chung, Y. D. (2021). Successive Point-of-Interest Recommendation With Local Differential Privacy. *IEEE Access*, *9*, 66371. https://doi.org/10.1109/access.2021.3076809.

Lee, H., & Kobsa, A. (2019). Confident Privacy Decision-Making in IoT Environments. *ACM Transactions on Computer-Human Interaction*, *27*(1), 1. https://doi.org/10.1145/3364223

Li, Y., Tan, Z., & Liu, Y. (2023). Privacy-Preserving Parameter-Efficient Fine-Tuning for Large Language Model Services. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2305.06212.

Lim, S., & Kim, M. (2025). AI-powered personalized recommendations and pricing: Moderating effects of ethical AI and consumer empowerment. *International Journal of Hospitality Management*, *130*, 104259. https://doi.org/10.1016/j.ijhm.2025.104259

Liu, A., Wang, W., Li, Z., Liu, G., Li, Q., Zhou, X., & Zhang, X. (2017). A Privacy-Preserving Framework for Trust-Oriented Point-of-Interest Recommendation. *IEEE Access*, *6*, 393. https://doi.org/10.1109/access.2017.2765317.

Lu, W., Zhang, J., Li, H., Li, C., & Su, Y.-J. (2025). The Influence of AI-Driven Personalization in Social Media Marketing on Consumer Purchase Decisions and Behavior. *International Journal of Accounting and Economics Studies*, *12*(5), 438. https://doi.org/10.14419/dcggbj32.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734. https://doi.org/10.2307/258792

Monzer, C., Moeller, J., Helberger, N., & Eskens, S. (2020). User Perspectives on the News Personalisation Process: Agency, Trust and Utility as Building Blocks. *Digital Journalism*, *8*(9), 1142. https://doi.org/10.1080/21670811.2020.1773291.

Moshed, A., & Al-Jabaly, S. M. (2024). Enhancing marketing success in Jordanian telecom: Strategic IoT integration and brand relationship management for maximized consumer loyalty. *Journal of Infrastructure Policy and Development*, *8*(6), 3858. https://doi.org/10.24294/jipd.v8i6.3858.

Nikiforov, L. (2024). Groups of Persons in the Proposed AI Act Amendments. *European Journal of Risk Regulation*, *15*(3), 757. https://doi.org/10.1017/err.2024.13.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T., Mulrow, C. D., Shamseer, L., Tetzlaff, J., Akl, E. A., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*. https://doi.org/10.1136/bmj.n71.

Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. *Penguin Press*. ISBN: 978-1594203008.

Reddi, V. J. (2025). *Generative AI at the Edge*. https://doi.org/10.1145/3733702.

Renda, A., Ducange, P., Marcelloni, F., Sabella, D., Filippou, M. C., Nardini, G., Stea, G., Virdis, A., Micheli, D., Rapone, D., & Baltar, L. G. (2022). Federated Learning of Explainable AI Models in 6G Systems: Towards Secure and Automated Vehicle Networking. *Information*, *13*(8), 395. https://doi.org/10.3390/info13080395.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393-404. https://doi.org/10.2307/259285.

Reusens, M., & Baesensa, B. (2025). *LLM Anthropomorphization: Balancing Ethics and Business Value*.

Seymour, W., & Such, J. M. (2022). Ignorance is Bliss? The Effect of Explanations on Perceptions of Voice Assistants. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2211.12900.

Sheth, A., Gaur, M., Roy, K., & Faldu, K. (2021). Knowledge-Intensive Language Understanding for Explainable AI. *IEEE Internet Computing*, *25*(5), 19. https://doi.org/10.1109/mic.2021.3101919.

Silalahi, A. D. K. (2025). Can generative artificial intelligence drive sustainable behavior? A consumer-adoption model for AI-driven sustainability recommendations. *Technology in Society*, *83*, 102995. https://doi.org/10.1016/j.techsoc.2025.102995.

Sun, Y., Freeman, J., Shoenberger, H., & Shen, F. (2025). To Tell or Not to Tell: Investigating the Persuasive Appeal of Information Transparency for AR-Powered E-Commerce Sites. *International Journal of Human-Computer Interaction*, 1. https://doi.org/10.1080/10447318.2025.2495847.

Tabaghdehi, S. A. H., & Arda, Ö. A. (2025). AI ethics in action: a circular model for transparency, accountability and inclusivity. *Journal of Managerial Psychology*. https://doi.org/10.1108/jmp-03-2024-0177.

Tran, M. T. (2025). Advancing retail and service strategies: AI-driven consumer behavior prediction, gamification, and ethical marketing. *Journal of Retailing and Consumer Services*, *88*, 104558. https://doi.org/10.1016/j.jretconser.2025.104558.

Virvou, M. (2023). Artificial Intelligence and User Experience in reciprocity: Contributions and state of the art. *Intelligent Decision Technologies*, *17*(1), 73. https://doi.org/10.3233/idt-230092.

Wahab, O. A., Rjoub, G., Bentahar, J., & Cohen, R. (2022). Federated against the cold: A trust-based federated learning approach to counter the cold start problem in recommendation systems. *Information Sciences*, *601*, 189. https://doi.org/10.1016/j.ins.2022.04.027.

Wang, J., Qiao, K., & Zhang, Z. (2018). Trust evaluation based on evidence theory in online social networks. *International Journal of Distributed Sensor Networks*, *14*(10). https://doi.org/10.1177/1550147718794629.

Wang, J., Tang, H., Man, S. S., Chen, Y., Zhou, S., & Chan, A. H. S. (2025). Critical Factors in Young People's Use and Non-Use of AI Technology for Emotion Regulation: A Pilot Study. *Applied Sciences*, *15*(13), 7476. https://doi.org/10.3390/app15137476.

Wang, S., Chen, Z., Xiao, Y., & Lin, C.-Y. (2021). Consumer Privacy Protection With the Growth of AI-Empowered Online Shopping Based on the Evolutionary Game Model. *Frontiers in Public Health*, *9*, 705777. https://doi.org/10.3389/fpubh.2021.705777.

Wang, Y. (2023). *TRUSTWORTHY AI AND DATA LINEAGE Balancing Trustworthiness and Efficiency in Artificial Intelligence Systems: An Analysis of Tradeoffs and Strategies*. https://doi.org/10.1109/MIC.2023.3303031.

WANG, Y., XU, Y., & ZHONG, Y. (2025). *Does Artificial Intelligence Invariably Enhance ESG Performance?*

Wu, H., Li, M., & Zhang, H. (2019). Enabling Smart Anonymity Scheme for Security Collaborative Enhancement in Location-Based Services. *IEEE Access*, *7*, 50031. https://doi.org/10.1109/access.2019.2911107.

Wu, W., Huang, Y., & Qian, L. (2023). Social trust and algorithmic equity: The societal perspectives of users' intention to interact with algorithm recommendation systems. *Decision Support Systems*, *178*, 114115. https://doi.org/10.1016/j.dss.2023.114115.

Xia, J., Yang, Y., Wang, S., Yin, H., Cao, J., & Yu, P. S. (2023). Bayes-Enhanced Multi-View Attention Networks for Robust POI Recommendation. *IEEE Transactions on Knowledge and Data Engineering*, *36*(7), 2895. https://doi.org/10.1109/tkde.2023.3329673.

Xu, H., Luo, X. R., 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. https://doi.org/10.1016/j.dss.2010.11.017.

Yan, W., Li, C., Huang, Y., & Yang, L. (2019). Low-Complexity Decentralized Recommendation System With Similarity Constraints. *IEEE Access*, *7*, 146922. https://doi.org/10.1109/access.2019.2946485.

Zhang, H., Wu, B. Y., Yuan, X., Pan, S., Tong, H., & Pei, J. (2024). Trustworthy Graph Neural Networks: Aspects, Methods, and Trends. *Proceedings of the IEEE*, *112*(2), 97. https://doi.org/10.1109/jproc.2024.3369017.

Ziller, C., Loepp, B., Kindermann, B., Köchling, G., & Fadeeva, Y. (2025). Willingness to share personal data online: The role of social influence and sustainability. *Technology in Society*, *83*, 102974. https://doi.org/10.1016/j.techsoc.2025.102974.