JMM17: Jurnal Ilmu Ekonomi dan Manajemen
Sinta 3 Accredited SK No. 72/E/KPT/2026
Journal page is avaliable to
https://jurnal.untag-sby.ac.id/index.php/jmm17/index

Consumer Behaviour Towards Privacy Personalization Trade Off in Digital Markets

Benazir Quadir[1], Yi Meng [2], Sumiati [3*]
[1,2] Xi'an Jiaotong-Liverpool University, China
[3]Universitas 17 Agustus 1945 Surabaya, Indonesia
Corresponding Author: sumiati@untag-sby.ac.id

ARTICLE INFO

Article history:
Submitted: 06-08-2026
Revised: 2-09-2026
Accepted: 20 September 2026

Keywords:
Privacy Paradox, Personalization, Consumer Behaviour, Digital Markets, Data Governance

Citing this article:
Benazir Quadir, Yi Meng , and Sumiati, 2026. Consumer Behaviour Towards Privacy Personalization Trade Off in Digital Markets. *JMM17: Jurnal Ilmu Ekonomi dan Manajemen*, vol. 12, no. 2, pp. 168-180, 2026.

ABSTRACT

Digital platforms increasingly employ data-driven personalization to shape consumer experiences and influence decision-making. Yet, the effectiveness of personalization depends on the collection, analysis, and profiling of personal data, creating an inherent tension between perceived consumer value and privacy concerns. This study examines consumer behaviour towards the privacy–personalization trade-off in digital markets, focusing on how consumers negotiate perceived benefits, privacy risks, trust, and autonomy in digital interactions. Using a qualitative interpretive approach, in-depth interviews were conducted with 25 active e-commerce users in Indonesia. The findings reveal three interrelated behavioural patterns: benefit-seeking behaviour, where personalization utility outweighs perceived privacy costs; conditional trust-dependent behaviour, where transparency, platform trustworthiness, and perceived control shape privacy acceptance; and risk-aware passive compliance, where consumers recognize privacy risks yet continue data disclosure due to convenience, limited alternatives, habitual use, and decision fatigue. These findings conceptualize the privacy–personalization trade-off not as a static preference or binary choice, but as a dynamic and context-dependent behavioural negotiation shaped by evolving perceptions of value, risk, trust, and control. The study extends understanding of digital consumer behaviour by revealing how these mechanisms jointly influence privacy-related decisions in an emerging digital market context. From a managerial and policy perspective, the findings underscore the importance of ethical personalization and user-centric privacy governance through greater transparency, meaningful consent, accessible privacy controls, and mechanisms that strengthen consumer agency without diminishing the benefits of personalized digital experiences.

2026 JMM17: Jurnal Ilmu Ekonomi dan Manajemen (Journal of Economic and Management Science) with CC BY NC SA license.

Introduction

Digital markets have become increasingly data-intensive, with consumer preferences and purchase decisions shaped by algorithmic and AI-enabled systems [28]. Digital platforms use behavioural analytics and machine learning to deliver personalized recommendations, targeted advertising, and customized offers that improve relevance and engagement [18]; [20]; [33]. Personalization has consequently become an important mechanism for enhancing customer experience, engagement, and recommendation acceptance [33]; [26]. Such personalization can also reduce consumers' information-processing effort and enhance recommendation acceptance [26]; [33]. However, these benefits depend on extensive collection and profiling of personal data, raising concerns

over privacy, surveillance, data misuse, and loss of control [11]; [25]. Accordingly, personalization is increasingly viewed as both value-enhancing and privacy-sensitive [5]; [37].

This tension is commonly described as the privacy–personalization trade-off, where consumers value tailored digital experiences while remaining concerned about the use of their personal information [21]. Privacy calculus theory suggests that consumers weigh expected benefits against perceived privacy risks [24]. Yet disclosure decisions are not purely rational; trust, perceived control, emotional attachment, platform experience, and contextual factors also shape consumer responses [26]; [5]. Consumers may therefore continue sharing data despite privacy concerns, reflecting the privacy–behaviour gap [29]. Habitual platform use, convenience, and consent fatigue may further reinforce such behaviour [2].

This paradox is particularly pronounced in mobile-first economies such as Indonesia, where rapid digital adoption may outpace data literacy and the development of effective protective frameworks. Consumers may consent to extensive data practices in exchange for lower prices, exclusive offers, seamless experiences, or platform loyalty benefits [14]. Consequently, privacy compromises may be rationalized as a necessary value exchange rather than primarily as an ethical concern. Indonesia is also the largest digital economy in Southeast Asia, with e-commerce remaining a major driver of digital growth [17]. Rapid digitalisation, AI-enabled marketing, and varying levels of awareness of data governance, therefore, make Indonesia an important setting for examining privacy-related consumer behaviour [9].

Despite substantial scholarship on online privacy and data protection, important gaps remain. Much of the privacy calculus literature conceptualizes information disclosure as a structured assessment of perceived benefits and risks, although recent research shows that personalization-related decisions also involve trust, control, emotions, habits, and contextual influences [5]; [37]. Similarly, existing studies often frame disclosure as a rational risk–benefit decision, whereas behavioural perspectives emphasize the roles of social norms, framing, trust, and platform persuasion [1]; [19]. Moreover, empirical research has predominantly relied on quantitative models, providing limited insight into how consumers themselves interpret and negotiate these tensions in everyday digital interactions. Consumer privacy scholarship also remains disproportionately grounded in Western contexts, with comparatively limited attention to Southeast Asian consumers and culturally specific privacy behaviours [22]. Within Indonesia, although emerging studies have examined AI personalization, privacy risk, trust, and behavioural outcomes, qualitative understanding of the lived behavioural processes underlying the privacy–personalization trade-off remains comparatively underdeveloped.

Addressing these gaps, this study conceptualizes the privacy–personalization trade-off as a dynamic and context-dependent behavioural negotiation rather than a one-time disclosure decision. Using a qualitative interpretive approach, it examines how Indonesian e-commerce consumers negotiate perceived value, privacy risks, trust, autonomy, and control in everyday digital interactions. In addition, Indonesia provides a relevant context because of its rapid e-commerce growth, expanding use of AI-driven marketing, and varying levels of consumer awareness regarding data governance [30].

Accordingly, the study addresses the following research questions:

RQ1. How do consumers interpret and negotiate the trade-off between personalization benefits and perceived privacy risks in digital markets?

RQ2. What behavioural and contextual factors shape consumers' willingness to disclose personal information in exchange for personalized digital experiences?

RQ3. How do trust, transparency, perceived control, and autonomy influence consumers' privacy-related decisions?

The study contributes theoretically by extending privacy calculus and privacy–personalization research through a behavioural negotiation perspective. Empirically, it provides qualitative evidence from Indonesia, while practically it informs ethical personalization, transparent data practices, meaningful consent, and stronger consumer control.

Personalization as a Digital Market Value Proposition

Personalization has become a central feature of digital platforms across e-commerce, streaming, travel, and social commerce ecosystems. AI-driven recommendation systems analyze behavioural and contextual data to deliver more relevant offers, improve browsing efficiency, and support purchase decisions [20]; [33]. Personalized recommendations can also enhance perceived usefulness, trust, and purchase intention when consumers understand how recommendations are generated [34]. More broadly, personalization reduces information-processing effort and can strengthen perceived value, engagement, and platform loyalty through convenience and service relevance [16]; [26].

However, these benefits depend on extensive data profiling, behavioural tracking, and predictive analytics, raising concerns about privacy intrusion, manipulation, and loss of autonomy [5]. Evidence further suggests that consumer acceptance increases when users retain greater autonomy over algorithmic recommendations [10]. Personalization should therefore be viewed not only as a marketing optimization strategy but also as a form of algorithmic behavioural influence shaping consumer choice and platform–consumer relationships.

Privacy Concerns and the Consumer Data Economy

Digital markets increasingly operate through a data-for-service exchange, where consumers disclose personal information in return for convenient and personalized services. However, such exchanges expose users to risks including unauthorized data use, security breaches, profiling, algorithmic opacity, and loss of informational control [7]; [23]. These concerns are intensified as AI-enabled platforms rely on increasingly granular consumer data to improve personalization and service accuracy [38].

The complexity of platform ecosystems also limits consumers' understanding of how data are collected, shared, and monetized, raising concerns about data ownership and platform power [35]. In Indonesia, the Personal Data Protection (PDP) Law provides a formal framework for strengthening privacy rights; however, effective protection remains dependent on enforcement, consumer data literacy, transparency, and implementation capacity [15]; [27]. Such asymmetries can reinforce surveillance capitalism, in which platform value creation increasingly relies on consumer traceability, data extraction, and behavioural prediction.

Consequently, consumers face a psychological contradiction: they remain concerned about how companies collect and use their data yet continue disclosing personal information for convenience and digital participation. Such behaviour reflects not only privacy calculus but also trust, perceived benefits, affect, and platform design [8]; [38]. This contradiction reinforces the privacy paradox, whereby privacy concerns coexist with continued data disclosure.

The Privacy Personalization Paradox

The privacy–personalization paradox reflects the tension between consumers' desire for personalized digital experiences and their concerns about disclosing personal information. Although consumers express privacy concerns, they often continue sharing data when perceived benefits—such as convenience, relevance, and personalized value—outweigh anticipated privacy risks [26]; [33]. Recent research further suggests that this trade-off extends beyond a purely rational privacy calculus and is shaped by trust, perceived control, platform experience, and contextual factors [5].

This attitude–behaviour inconsistency may also arise from convenience, perceived value, limited control, and privacy cynicism, which encourage continued disclosure despite privacy awareness [37]. Trust is particularly important, as consumers' willingness to disclose data increases when platforms are perceived as trustworthy and reciprocal [26]. In social commerce, information sharing, social support, trust, and perceived privacy risk further interact in shaping consumer behaviour [5].

Accordingly, the privacy–personalization paradox should be understood as a dynamic and context-dependent behavioural negotiation, rather than a simple rational trade-off. Recent systematic evidence similarly emphasizes the need for more user-centric explanations of how consumers navigate personalization benefits and privacy concerns [12].

Behavioural Economics and Bounded Rationality

Traditional privacy calculus assumes that consumers evaluate data disclosure by weighing perceived benefits against anticipated risks. However, recent research suggests that privacy-related decisions are often shaped by bounded rationality, whereby consumers rely on simplified judgments, affect, habits, and contextual cues rather than fully deliberative evaluation [5]; [26]. Immediate personalization benefits, such as convenience, relevance, and reduced search effort, may therefore outweigh uncertain or delayed privacy consequences [33].

Behavioural tendencies such as present-oriented preferences, optimism about personal vulnerability, and reliance on platform cues can further normalize disclosure. Recent experimental evidence also shows that positive affect can increase consumers' willingness to disclose sensitive information despite perceived privacy risks [8]. At the same time, greater decisional autonomy increases acceptance of algorithmic recommendations, highlighting the importance of perceived control in digital choice environments [10]. Thus, the privacy–personalization trade-off reflects a bounded, context-dependent, and behaviourally influenced decision process, rather than a purely rational cost–benefit calculation.

Socio Technical Systems and Power Dynamics

AI-driven digital platforms shape consumer behaviour through the interaction of technological design, algorithmic governance, and social context. Recommendation systems do not merely predict preferences; they also structure available options, frame choices, and influence perceived autonomy [31]. Recent research shows that consumer acceptance of AI-assisted decisions depends strongly on perceived choice and decision autonomy [10]; [13].

From a socio-technical perspective, privacy behaviour is therefore shaped by interface design, algorithmic authority, platform governance, and socially normalized digital practices. Online choice architectures and dark patterns can exploit behavioural biases, steer consent, and weaken consumer agency [3]; [32]. Empirical evidence further demonstrates that manipulative interface designs can influence consumers across different vulnerability groups [36]. Thus, privacy decisions emerge through a co-production between consumers and algorithmic systems, within an asymmetric platform environment where technological design can subtly constrain meaningful choice and control.

Method

Research Paradigm

This study adopts a descriptive–interpretative research paradigm, recognising that consumers' decisions regarding privacy–personalization trade-offs are shaped by subjective meaning-making processes, behavioural negotiation, and contextual influences. Rather than conceptualising privacy-related decisions as purely objective calculations of risks and benefits, the interpretative perspective views consumer behaviour as socially constructed and psychologically negotiated through ongoing interactions with digital platforms [6].

From this perspective, reality is understood through participants' lived digital experiences. Consumers may simultaneously recognise the risks associated with data disclosure while continuing to engage with personalized digital services because of perceived convenience, relevance, economic benefits, or habitual platform use. Accordingly, perceptions of personalization benefits, privacy risks, trust, and control are not regarded as fixed evaluations; instead, they are continuously interpreted and renegotiated within specific digital and social contexts.

Research Approach and Design

A qualitative descriptive research design was employed to explore the behavioural patterns, perceptions, and interpretative reasoning underlying consumers' personal-data disclosure practices in digital markets. This design was considered appropriate because the study seeks to understand not only what consumers do when confronted with privacy–personalization trade-offs, but also how they explain, justify, and make sense of these behaviours.

The qualitative approach enables an in-depth examination of how consumers perceive personalization benefits, interpret privacy implications, and rationalize continued engagement with data-intensive digital platforms. Particular attention is given to tacit emotional responses, habitual and normalized behaviours, perceived convenience, trust, autonomy, and the cognitive frames through which consumers evaluate data disclosure. The design therefore facilitates a contextualised understanding of privacy-related behaviour that may not be adequately captured through predetermined quantitative measures alone.

Research Context

Indonesia offers a relevant setting for examining privacy–personalization trade-offs due to its rapidly growing digital economy, mobile-first adoption, and widespread use of AI-driven personalization across e-commerce and social-commerce platforms. East Java was selected because of its diverse digital-consumer population, varying levels of digital literacy, and active engagement with online commerce. Participants from urban, peri-urban, and less densely populated areas, including Surabaya, Malang, and Banyuwangi, enabled the study to capture varied privacy perceptions and disclosure behaviours across different socioeconomic and digital contexts.

Participants and Sampling Strategy

The study involved 25 digitally active consumers aged 18–35 years who made online purchases at least twice per month. Purposive sampling was used to recruit participants who regularly encountered personalized recommendations, used multiple digital platforms, and had some awareness of privacy, tracking, consent, or data collection. Variation in gender, digital literacy, platform use, and consumption patterns was sought to capture diverse behavioural interpretations rather than achieve statistical representativeness.

Data Collection Procedures

Data were collected through semi-structured, in-depth interviews lasting approximately 25–45 minutes. The interviews explored perceptions of personalization benefits, awareness of data tracking and privacy practices, experiences of consent and trust, motivations for privacy concessions, and perceptions of autonomy and digital risk.

Interviews were conducted face-to-face or online, depending on participant preference. Probing questions were used to clarify responses and explore underlying motivations. With participants' consent, interviews were recorded, transcribed verbatim, and prepared for qualitative analysis to identify recurring behavioural patterns and interpretations of privacy–personalization trade-offs.

Data Analysis Strategy

The data were analysed using NVivo-assisted thematic analysis to identify recurring patterns across participants' narratives. Analysis proceeded through three coding stages: open coding to identify descriptive meaning units, axial coding to group related behavioural and interpretive categories, and selective coding to develop overarching themes explaining how consumers negotiate privacy–personalization trade-offs.

Analytical rigor was supported through peer debriefing, iterative code refinement, and analytical memoing. Thematic saturation was reached after 23 interviews, with the final two interviews used to confirm coding stability and thematic completeness. NVivo functions, including coding queries, word-frequency analysis, and thematic mapping, were used to enhance analytical transparency and consistency.

Results and Discussion

Qualitative analysis revealed four interconnected themes shaping consumer behavioural negotiation of the privacy personalization trade off in digital markets. Users demonstrate

rationalization patterns where convenience, trust, and social normalization outweigh concerns on autonomy loss and data misuse.

Benefit Driven Dependency on Personalization

Consumers predominantly frame data disclosure as a value exchange, where convenience, efficiency, and promotional benefits outweigh privacy anxiety. Many participants emphasized the time saving value of personalization, describing tailored recommendations as a core feature that enhances daily productivity.

"Why waste time searching if the app already knows what I like?" (P07)

Platforms are perceived as personal assistants, guiding consumption decisions easier and faster, particularly in fast paced digital lifestyles among Indonesian youth.

Furthermore, personalization is financially rewarding. Cashback features, discounts, free shipping, and personalized bundle promotions encourage users to willingly provide their data.

"I give my data because promo is worth the sacrifice." (P11)

This behaviour shows strong alignment with prospect theory, where immediate rewards overshadow future losses [39].

Another rationalization mechanism is emotional satisfaction. Personalized interfaces create a sense of recognition and emotional attachment, making the digital shopping experience feel tailored and exclusive. Personalization thus becomes a driver of habitual loyalty, embedding continuous consent into routine platform usage.

➞ Interpretive meaning:

Consumers normalize privacy risk because personalization feels beneficial, harmless, and necessary for digital participation.

Trust Based Disclosure and Legitimization

Trust acts as a primary defence line in privacy negotiations. Users rely on assumptions that popular brands are safe, rather than understanding actual data protection mechanisms.

"I trust big companies, if they cheat us pasti ketahuan." (P18)

Trust simplifies decision making, reducing cognitive load when interacting with complex data permissions. Participants frequently equated longevity of brand usage and positive past experience with data security assurance.

"I've been using Shopee and Gojek for years, so I feel protected." (P04)

This phenomenon reflects trust heuristics, where people form judgments based on familiarity instead of evidence.

Peer influence also reinforces legitimacy:

if everyone in a social circle uses the same app, perceived risk becomes socially minimized.

"Kalau semua teman juga pake, aman lah." (P12)

Trust also shields platforms from blame. When privacy breaches occur, users attribute responsibility to hackers rather than the companies.

➞ Interpretive meaning:

Trust does not just reduce concern

it creates blind tolerance, letting platforms maintain data dominance without accountability pressure.

Passive Compliance and Consent Fatigue

Consumers experience mental exhaustion from repetitive consent notifications and complex privacy settings. Policies are seen as intentionally designed to confuse and discourage critical evaluation.

"Kebanyakan tulisan… udah, allow aja." (P21)

This generates automatic behavioural scripts: users click "Agree" without reading.

Some participants expressed feelings of coercion:

"Kalau ga izinkan semua data, aplikasinya ga bisa dipake." (P10)

This indicates structural unfairness, where privacy choice is an illusion apps gatekeep access until data is surrendered.

Additionally, UI nudges highlighted buttons, forced scrolling steer users to the most data invasive option. These dark patterns transform consent into manipulated compliance, not voluntary agreement.

➞ Interpretive meaning:

Consumers do not "choose" to reveal data

they are guided and worn down to comply.

Risk Awareness Without Behavioural Change

Participants demonstrated high conceptual awareness of privacy risks, particularly regarding financial fraud and identity theft. However, this knowledge does not trigger preventive actions.

"I know the danger… but offline life is too hard now." (P15)

Risk becomes secondary when functionality is required for:

1. Transport
2. Payments
3. Shopping
4. Entertainment
5. Communication

Digital market dependency produces no viable alternatives.

"Semua sudah digital, resiko diterima aja." (P02)

Users apply optimism bias believing bad outcomes are unlikely for themselves

➞ Interpretive meaning:

Risk awareness creates emotional discomfort,

but behaviour stays unchanged because digital exclusion is worse.

Integrated Interpretation and Theoretical Alignment

Combining all themes demonstrates that consumer privacy decisions are shaped by behavioural emotion, platform control, and collective normalization not rational evaluation.

Table 1. Supporting theories from literature

Theory	How it explains findings
Behavioural Economics	Rewards > future threats
Socio Technical Systems	Platforms shape decision pathways
Interpretivism	Meaning making > objective facts
Privacy Paradox	Concern ≠ action

Thus, privacy personalization negotiation is a continuously reinterpreted social process, driven by:

1. contextual urgency
2. trust shortcuts
3. systemic coercion
4. digital lifestyle pressure

Table 2. Thematic Map of Consumer Privacy Behaviour

Theme	Behavioural Meaning	Core Driver	Implication
T1	Data sharing = value exchange	Convenience incentives	Privacy becomes transactional
T2	Trust short circuits risk evaluation	Familiarity & social proof	Blind acceptance of platform power
T3	Reluctant consent becomes habitual	Dark UX & fatigue	Autonomy loss normalized
T4	Awareness ≠ action	Digital necessity	Permanent privacy compromise

Figure 1. Interpretive Behavioural Negotiation Loop

Personalization Rewards

↓

Trust & Familiarity

↓

Passive Compliance

↓

Risk Awareness

↓

(Back to Personalization Rewards → loop continues)

Summary of Findings

The thematic analysis demonstrates that consumers do not evaluate privacy personalization trade offs using rational risk assessment, but through interpretive behavioural reasoning rooted in everyday digital dependence. Personalization benefits generate emotional gratification and functional reliance, encouraging habitual data sharing. Trust in platform credibility acts as a psychological justification that validates continuous disclosure without demanding transparency. Meanwhile, passive compliance emerges from persuasive design structures, transforming consent into a default behavioural pathway.

Although participants demonstrate awareness of potential data exploitation, this recognition does not translate into resistance because digital exclusion is perceived as a greater threat than privacy loss. Users experience structural coercion in which "opting out" is not a real choice, reinforcing acceptance of surveillance norms.

Consequently, the findings confirm that consumer privacy decisions occur within a socio technical loop where convenience, trust, and interface persuasion reduce the influence of risk awareness. Data disclosure becomes culturally normalized, materially incentivized, and behaviourally embedded shaping privacy as a recurring negotiation rather than a conscious informed decision.

DISCUSSIONS

Rethinking the Privacy Personalization Trade Off through an Interpretive Behavioral Lens

The findings indicate that consumers view personalization not as a risky trade off, but as a necessary enhancement to everyday digital convenience. Rather than rationally balancing benefits and privacy threats, participants internalize personalization as a default consumption norm, framing data sharing as a normal and harmless part of digital life. This demonstrates that privacy concerns do not disappear; they are actively reinterpreted to justify ongoing participation in systems designed for data extraction.

Such behavior confirms that consumers make sense of personalization through emotionally grounded interpretations, where efficiency, relevance, and comfort dominate any future oriented anxiety. Privacy is accepted as something that can be "managed later" because immediate advantages feel more real than potential harms. Hence, privacy personalization becomes less of a conscious decision and more of a continuous behavioral adaptation within socio technical environments.

Integrating Behavioral Decision Theory and Socio Technical Influence

The privacy paradox is better understood when behavioral decision making and platform design are analyzed together. Consumers apply heuristics trust, social conformity, and simplicity to reduce cognitive effort during digital interaction. Meanwhile, platforms create architectures of compliance through persuasive interface design, optimizing user flow to prioritize consent and data extraction as the fastest route to product access.

This means privacy surrender does not solely come from personal choice, but from the way systems are built. Users are nudged, fatigued, or cornered into sharing personal data due to convenience and limited alternatives. Therefore, the trade off is the output of power dynamics, where platform design silently governs user autonomy.

Trust, Legitimization of Data Sharing, and Digital Dependency

Trust in platform reputation and widespread adoption leads consumers to believe security measures must be reliable. Familiarity becomes evidence, even without verification. The role of trust here is crucial: it legitimizes data risks and grants platforms freedom from constant scrutiny.

Digital dependency further deepens this dynamic. Users report that refusing data sharing results in loss of access to mobility, delivery, payment, or social participation. Thus, privacy is conceptualized as expendable when compared to operational needs of modern life.

Responsible Personalization as a Governance Objective

The findings call for a shift in personalization governance from extractive value capture to ethical co created value. Personalization should respect boundaries and reduce manipulative profiling. Transparent data use, control mechanisms, and informed interface standards are necessary to ensure personalization enhances not compromises consumer dignity.

Responsible personalization is achievable when algorithms are aligned with user empowerment, not merely behavioral targeting. This requires accountability regimes where platforms must justify data relevance, retention rationale, and fairness in algorithmic decision making.

Theoretical Contributions

This study contributes to several theoretical perspectives on digital consumer behaviour. It extends privacy paradox theory by conceptualizing privacy-related behaviour as a cyclical process of adaptation rather than a simple inconsistency between attitudes and actions. It also advances interpretivist consumer research by showing how surveillance and data disclosure become culturally normalized through repeated digital engagement. From a socio-technical perspective, the findings demonstrate that privacy decisions are shaped not only by individual preferences but also by interface design, default settings, and platform architecture. In addition, the study contributes to behavioural economics by illustrating how consumers tend to discount abstract and future privacy risks in favour

of immediate experiential benefits such as convenience, relevance, and personalization. Overall, the findings suggest that privacy choices are embedded within broader structures of platform power and should not be understood solely as expressions of individual preference.

Managerial Implications

The findings indicate that managers should redesign personalization practices around transparency, user autonomy, and responsible data use. Organizations should simplify consent processes, provide users with greater control over data collection and withdrawal, and adopt contextual personalization practices that minimize excessive tracking. Trust can also be strengthened through transparent accountability reporting and clear communication about how personal data are collected and used. At the same time, firms should establish ethical boundaries around persuasive technologies and behavioural profiling to reduce the risk of manipulation. Businesses that embed autonomy, transparency, and reversibility into personalization strategies are more likely to strengthen consumer trust and achieve long-term brand legitimacy in increasingly regulated digital markets.

Policy Directions and Future Agenda

The findings highlight several important policy priorities for strengthening consumer protection in digital markets. Regulators should address dark patterns and coercive consent practices, establish stronger requirements for algorithmic auditing and data-breach accountability, and ensure that consumers can exercise data portability and control without penalty or loss of essential services. Greater investment in digital-rights education is also needed to improve public understanding of privacy, consent, and data-driven decision-making. Future research should extend this work by examining cross-cultural differences in privacy behaviour, longitudinal changes in trust and autonomy, the implications of emotional AI and biometric surveillance, and the exposure of vulnerable populations to data-related risks. Overall, the findings suggest that sustainable digital markets require structural safeguards and institutional accountability rather than relying solely on consumers to make fully informed privacy decisions.

Conclusions

Concluding Synthesis

This study shows that consumer responses to privacy–personalization trade-offs are shaped less by rational calculation than by continuous negotiation within everyday digital life. Personalization provides immediate benefits such as convenience, relevance, speed, and ease of use, whereas privacy risks are often perceived as distant or abstract.

Consumers therefore normalize personal data disclosure as a condition of participation in digital commerce and social interaction. In this context, consent is not always fully autonomous but is shaped by platform design, behavioural heuristics, and limited alternatives. Privacy-related behaviour is thus better understood as an adaptive response to algorithmic environments rather than as simple inconsistency.

Theoretical and Practical Contributions

The study extends privacy paradox theory by showing that consumers are not necessarily irrational or contradictory; instead, they develop justifications that reconcile privacy concerns with dependence on digital services. This reframes the privacy paradox as a process of behavioural adaptation and normalization.

The findings also contribute to interpretivist consumer theory by demonstrating that privacy decisions are influenced by cultural meanings associated with convenience, modernity, and digital participation. In addition, the study supports a socio-technical perspective by showing how recommendation systems, interface design, and default settings can structurally shape perceived autonomy and choice.

Practically, the findings suggest that personalization should be based on transparent and responsible value creation rather than unilateral data extraction. Clear consent mechanisms, reduced

use of manipulative design, and stronger explanations of data use may enhance consumer trust, legitimacy, and long-term platform relationships.

Policy Recommendations

The findings highlight the need for more agency-centred digital regulation, particularly in emerging digital economies. Policy should address power imbalances between platforms and consumers by promoting transparent consent, restricting deceptive interface practices, strengthening algorithmic accountability, supporting effective redress mechanisms, and enhancing data portability.

Regulation should therefore move beyond data protection alone and place greater emphasis on consumer autonomy, dignity, and meaningful choice. Protecting these principles is essential for sustaining trust and fairness in increasingly data-driven markets.

Future Research Directions

Future research should examine privacy–personalization behaviour across broader demographic groups, including older adults, rural consumers, and individuals with lower digital literacy. Longitudinal studies could also investigate how major data breaches, regulatory changes, or evolving platform practices influence privacy behaviour over time.

Further studies may compare different digital environments, such as social media, financial services, healthcare applications, and e-commerce platforms, where perceptions of data sensitivity may vary. Combining qualitative methods with digital trace data may also provide deeper insight into the relationship between stated privacy preferences and actual behaviour. Emerging issues such as biometric surveillance, emotion AI, and predictive profiling warrant particular attention.

Final Reflection

Personalization can improve convenience and decision-making, but it may also reshape consumer autonomy in subtle ways. This study suggests that users often accept surveillance because digital platforms make data disclosure increasingly difficult to avoid. A sustainable digital ecosystem therefore requires personalization practices that preserve human agency, transparency, and meaningful consent. Privacy should not be treated as the price of convenience, but as a fundamental condition of responsible digital innovation.

1. References

[1] Barth, S., & De Jong, M. D. (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

[2] Bietti, E. (2020). Consent as a free pass: platform power and the limits of the informational turn. Pace Law Review, 40(1), 310. https://doi.org/10.58948/2331-3528.2013

[3] Brenncke, M. (2024). A Theory of Exploitation for Consumer Law: Online choice architectures, dark patterns, and autonomy violations. Journal of Consumer Policy, 47(1), 127–164. https://doi.org/10.1007/s10603-023-09554-7

[4] Shalini, R. C. (2025). The influence of AI-Powered Recommendation Systems on consumer choice. International Journal for Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.43571

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

[6] Creswell, J., Poth, C. N., & Rawlins, P. (2023). Mapping design trends and evolving directions using the Sage handbook of mixed methods research design. SAGE handbook of mixed methods research design, 527-537.

[7] De Capitani Di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2020). Toward owners' control in digital data markets. IEEE Systems Journal, 15(1), 1299–1306. https://doi.org/10.1109/jsyst.2020.2970456

[8] Demmers, J., Dellaert, B. G. C., & Rotaru, K. (2025). Consumer Financial Self-Disclosure Online: Positive affect Trumps perceived privacy risks in personal customer portals. Journal of the Association for Consumer Research, 10(3), 277–289. https://doi.org/10.1086/735022
[9] Fatmawati, E., A, A. N. M. a. S., Rafa, M. F. F., Sari, A. R., & Hasibuan, M. (2025). Digital rights regulation in the AI era: privacy protection and consumer rights in Indonesia. Journal of Social and Economics Research, 7(2), 1780–1792. https://doi.org/10.54783/jser.v7i2.1344
[10] Fink, L., Newman, L., & Haran, U. (2024). Let me decide: Increasing user autonomy increases recommendation acceptance. Computers in Human Behavior, 156, 108244. https://doi.org/10.1016/j.chb.2024.108244
[11] Gambs, S. (2019). Privacy and ethical challenges in big data. Lecture Notes in Computer Science, 17–26. https://doi.org/10.1007/978-3-030-18419-3_2
[12] Hsu, M., Parry, G., & Ng, I. (2026). Personalisation-Privacy paradox: Systematic review and survey evidence on personal data stores. Expert Systems, 43(7). https://doi.org/10.1111/exsy.70314
[13] Husairi, M. A., & Rossi, P. (2023). Delegation of purchasing tasks to AI: The role of perceived choice and decision autonomy. Decision Support Systems, 179, 114166. https://doi.org/10.1016/j.dss.2023.114166
[14] Hutabarat, H. P. L., Edgarian, J., & Hellyani, C. A. (2026). Kajian Literatur atas Dinamika Isu Privasi Data dan Kepercayaan pada pengguna E-Commerce di Indonesia. Maslahah Jurnal Manajemen Dan Ekonomi Syariah, 4(3), 18–29. https://doi.org/10.59059/maslahah.v4i3.3090
[15] Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. The Easta Journal Law and Human Rights , 3(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351
[16] Julina, J., Nurlasera, N., Miftah, D., & Zahirah, Q. R. (2026). Beyond the algorithm: the mediating role of perceived value in driving customer loyalty. International Conference on Business Management and Accounting, 4(1), 41–52. https://doi.org/10.35145/icobima.v4i1.5300
[17] Jumiati, Rosdiana, H., & Kusumastuti, R. (2017). The protection of information privacy in Indonesia's e-commerce: A Legal approach perspective. KnE Social Sciences, 2(4), 59. https://doi.org/10.18502/kss.v2i4.868
[18] Kapoor, P. (2019). Consumer Data Analytics for personalized digital marketing. International Journal of Commerce Finance and Digital Economy, 2, 1–16. https://doi.org/10.67228/3071642x/ijcfde-2019pii9p6w
[19] Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal, 25(6), 607–635. https://doi.org/10.1111/isj.12062
[20] Kim, S., Lee, S., Biswas, D., Shahnawaj, M., Kyoom, N. M., & Bhardwaj, P. (2025). Personalization and recommendation systems: leveraging machine learning algorithms to offer personalized product recommendations and content to customers based on their behavior, preferences, and purchasing history. International Journal of Grid Computing & Applications, 16(2), 1–4. https://doi.org/10.5121/ijgca.2025.16201
[21] Kobsa, A. (2007). Generic user modeling systems. Lecture Notes in Computer Science, 136–154. https://doi.org/10.1007/978-3-540-72079-9_4
[22] Kumar, A., Shankar, A., Behl, A., Chakraborty, D., & Gundala, R. R. (2025). Anthropomorphic generative AI chatbots for enhancing customer engagement, experience and recommendation. Journal of Consumer Marketing, 42(4), 472–483. https://doi.org/10.1108/jcm-06-2024-6922
[23] Larsson, S. (2018). Algorithmic governance and the need for consumer empowerment in data-driven markets. Internet Policy Review, 7(2). https://doi.org/10.14763/2018.2.791
[24] Majumdar, A., & Bose, I. (2016). Privacy Calculus Theory and its applicability for emerging technologies. Lecture Notes in Business Information Processing, 191–195. https://doi.org/10.1007/978-3-319-45408-5_20

[25] Mazzarello, M., Duarte, F., Mora, S., Heine, C., & Ratti, C. (2025). Data Slots: trade-offs between privacy concerns and benefits of data-driven solutions. Humanities and Social Sciences Communications, 12(1). https://doi.org/10.1057/s41599-025-04776-1
[26] McKee, K. M., Dahl, A. J., & Peltier, J. W. (2024). Gen Z's personalization paradoxes: A privacy calculus examination of digital personalization and brand behaviors. Journal of Consumer Behaviour, 23(2), 405–422. https://doi.org/10.1002/cb.2199
[27] Pratiwi, B., Fadilla, N. N., Syawal, I. N., & Zholanda (2025). The Implementation of Personal Data Protection Policy within Indonesia's Digital Legal System. Perkara., 3(2), 844–859. https://doi.org/10.51903/2r46zv36
[28] Putra, P. M. (2026). The role of big data and artificial intelligence in shaping consumer preferences in the digital market. Nomico., 3(2), 33–45. https://doi.org/10.62872/ddgf9h80
[29] Reynolds, B., Venkatanathan, J., Gonçalves, J., & Kostakos, V. (2011). Sharing ephemeral information in online social networks: privacy perceptions and behaviours. Lecture Notes in Computer Science, 204–215. https://doi.org/10.1007/978-3-642-23765-2_14
[30] Tio, L., Kulal, S. M., Yadewani, D., & Nanda, A. P. (2026). AI-driven marketing personalization and customer engagement: an empirical investigation of the mediating roles of perceived value and customer trust. Jurnal Ilmiah Ilmu Terapan Universitas Jambi|JIITUJ|, 10(3), 1729–1741. https://doi.org/10.22437/jiituj.v10i3.56421
[31] Tuomi, T., Kaur, A., & Jones, V. (2022). Ethical dimensions of AI personalization. International Journal of Human Computer Studies, 166, 102932. https://doi.org/10.1016/j.ijhcs.2022.102932
[32] Trzaskowski, J. (2024). Manipulation by design. Electronic Markets, 34(1). https://doi.org/10.1007/s12525-024-00699-y
[33] Wang, Y., Zhu, J., Liu, R., & Jiang, Y. (2024). Enhancing recommendation acceptance: Resolving the personalization–privacy paradox in recommender systems: A privacy calculus perspective. International Journal of Information Management, 76, 102755. https://doi.org/10.1016/j.ijinfomgt.2024.102755
[34] Weidig, J., & Kuehnl, C. (2023). Improving the effectiveness of personalized recommendations through attributional cues. Psychology and Marketing, 40(12), 2559–2575. https://doi.org/10.1002/mar.21914
[35] Xi, X., Zhang, Y., & Goh, M. (2024). Consumer data collection strategies in two-sided platforms: The role of data ownership assignment and privacy concerns. International Journal of Production Economics, 280, 109435. https://doi.org/10.1016/j.ijpe.2024.109435
[36] Zac, A., Huang, Y., Von Moltke, A., Decker, C., & Ezrachi, A. (2025). Dark patterns and consumer vulnerability. Behavioural Public Policy, 1–50. https://doi.org/10.1017/bpp.2024.49
[37] Zhang, J. H., Koivumäki, T., & Chalmers, D. (2024). Privacy vs convenience: Understanding intention-behavior divergence post-GDPR. Computers in Human Behavior, 160, 108382. https://doi.org/10.1016/j.chb.2024.108382
[38] Zhou, T., & Tang, B. (2025). Examining user information disclosure on artificial intelligence-generated content platforms: A privacy calculus perspective. Information Development. https://doi.org/10.1177/02666669251384288