



Data Privacy and Consumer Trust in Digital Advertising Personalization: A Systematic Literature Review

Sahnidar Hasan^{1A-E*}, Irman^{2B-D}, Sukriadi^{3B-D}

^{1,2,3} Universitas Muhammadiyah Mamuju, Kota Mamuju, Indonesia

Email Corresponding Author: sahnidar.hs@gmail.com^{1*}

Authors' Contribution:

A. Conception and design of the study; B. Acquisition of data; C. Analysis and interpretation of data; D. Manuscript preparation; E. Obtaining funding

Received: 2026-06-23

Revised: 2026-07-14

Accepted: 2026-07-27

ABSTRACT

The expansion of data-driven advertising enables firms to deliver increasingly relevant messages, yet the collection, inference, and exchange of personal information may generate privacy concerns and weaken consumer trust. This study aims to systematically synthesize conceptual and empirical evidence concerning the relationships among data privacy, consumer trust, and personalized digital advertising, while identifying the conditions under which personalization produces acceptance or resistance. A systematic literature review was conducted using Scopus and Web of Science following the PRISMA 2020 framework. Searches covered peer-reviewed publications from 2016 to 2026 and combined keywords related to data privacy, trust, and advertising personalization. From 192 initially identified records, 148 titles and abstracts were screened, 40 full-text articles were evaluated, and 10 empirical studies published between 2017 and 2022 were included in the qualitative synthesis. The findings indicate that relevant and informative personalization can improve advertising attitudes, engagement, self-disclosure, and purchase responses when personal data are voluntarily supplied, contextually appropriate, transparently processed, and supported by meaningful consumer control. Conversely, covert tracking, third-party data sharing, sensitive inference, and privacy violations increase perceived vulnerability, erode trust, stimulate psychological reactance, and promote advertising avoidance or opt-out behavior. Conceptually, the synthesis integrates privacy calculus, contextual integrity, communication privacy management, psychological reactance, and trust theory, positioning trust as the principal mechanism linking data-governance practices to consumer responses. The study concludes that privacy protection is not merely a regulatory constraint but a strategic capability for achieving legitimate, sustainable, and effective personalization.

Keyword : Data Privacy; Consumer Trust; Digital Advertising; Advertising Personalization; Systematic Literature Review

INTRODUCTION

Digital advertising increasingly relies on consumer data including browsing histories, search behavior, location, purchase records, and inferred interests to deliver individually relevant messages. Such personalization can reduce information overload, improve advertising relevance, and facilitate consumer decision-making. Nevertheless, the same data-processing practices may create perceived surveillance, vulnerability, and loss of control. This tension constitutes the personalization–privacy paradox: consumers expect relevant digital experiences while simultaneously objecting to the collection and use of the data required to produce them (Boerman et al., 2017; Cloarec, 2020). Privacy calculus theory explains this tension as an evaluation of expected benefits against perceived privacy risks. Consumers may accept data collection



when personalization offers sufficient utility, convenience, or economic value. However, this calculation is neither entirely rational nor stable because it is influenced by limited knowledge, cognitive biases, contextual cues, and unequal information between consumers and platforms (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). Empirical evidence demonstrates that perceived benefits, privacy costs, and trust predict self-disclosure, although the magnitude of these relationships differs across commercial, news, and health environments (Bol et al., 2018).

Trust is therefore not simply an outcome of data practices but a central governance mechanism that enables consumers to accept vulnerability under conditions of uncertainty. Transparent and controllable data practices can reduce feelings of violation, whereas unauthorized access and privacy breaches weaken trust and subsequently damage behavioral and firm-level outcomes (Martin et al., 2017). Privacy violations can also initiate a negative spiral in which consumers become less willing to interpret subsequent organizational actions as competent or benevolent (Martin, 2018). Consequently, personalized advertising presents a strategic dilemma: increasing the depth of personalization may improve relevance but simultaneously reveal the extent of corporate surveillance, undermine trust, and stimulate advertising avoidance. The problem becomes more critical as algorithmic advertising systems infer sensitive characteristics rather than merely process information voluntarily provided by users. From the perspective of communication privacy management, consumers perceive personal information as something over which they retain ownership and expect legitimate boundaries governing access, transfer, and reuse. When advertisers cross informational or social boundaries, consumers may interpret personalization as an intrusion rather than a service (Zhu & Kanjanamekanant, 2021). Psychological reactance theory further suggests that perceived threats to autonomy generate resistance, avoidance, or efforts to restore control (Chen et al., 2019). Accordingly, the effectiveness of personalized advertising cannot be evaluated exclusively through click-through rates or purchase intentions; it must also be examined through privacy concerns, consumer trust, disclosure willingness, perceived control, and protective behavior.

Current scholarship recognizes personalized advertising as a double-edged mechanism. At the beneficial end, data-driven advertising increases message relevance and helps match consumers with suitable products. Aiolfi et al. (2021) found that perceived informativeness and entertainment can encourage responses to online behavioral advertising, whereas privacy and irritation risks may constrain these benefits. Zeng et al. (2021) likewise demonstrated that voluntary self-disclosure, privacy assurance, and an explicit personalization declaration can increase purchase responses to personalized promotions. These findings support privacy calculus theory by indicating that consumers may exchange data for recognizable value when the exchange is voluntary and understandable. At the adverse end, personalization may activate persuasion knowledge and alert consumers that their behavior is being monitored. Chen et al. (2019) showed that feelings of vulnerability and psychological ownership contribute to privacy concerns and reactance. Similarly, Morimoto (2021) found that information control and persuasion knowledge influence privacy concerns across social-media platforms. Personalized advertising is especially likely to cross consumer boundaries when it uses private information, involves third-party data sharing, or applies personalized pricing (Strycharz et al., 2019; Zhu & Kanjanamekanant, 2021).

Transparency and control have consequently emerged as important trust signals. Under signaling theory, privacy explanations, consent mechanisms, and preference controls communicate organizational accountability and reduce uncertainty. Nevertheless, transparency is conditional rather than universally beneficial. Kim et al. (2019) established that advertising transparency can improve effectiveness when it reveals acceptable information flows but can backfire when it exposes practices that violate consumers' contextual expectations. Privacy-control cues may also increase critical processing while simultaneously improving perceived persuasiveness, demonstrating that empowerment and skepticism can coexist (Zarouali et al., 2018). Recent studies have therefore shifted from asking whether personalization is effective to asking when, how, and for whom it is acceptable. Consumer-brand relationships, platform environments, data-collection methods, advertising literacy, and perceived control have been identified as boundary conditions (Hayes et al., 2022; Morimoto, 2021). Meanwhile, meta-analytical and review evidence indicates that privacy concern is associated with protective behavior, although its relationship with actual disclosure remains inconsistent (Baruh et al., 2017). This inconsistency reinforces the privacy paradox and warns against treating stated concern, behavioral intention, and observable behavior as equivalent constructs.

Despite substantial progress, the literature remains fragmented across advertising, information systems, marketing, communication, and privacy research. Existing reviews have classified the antecedents and outcomes of online behavioral advertising (Boerman et al., 2017) and mapped privacy research across advertising formats (Boerman & Smit, 2023). Reviews of the general privacy paradox

have also identified rational, bounded-rational, and behavioral explanations for discrepancies between stated preferences and behavior (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). However, these streams have not sufficiently integrated data privacy, consumer trust, and digital-ad personalization into a unified causal and contextual framework. Four limitations are particularly evident. First, privacy concern and trust are frequently examined as separate predictors, although trust may mediate, moderate, or dynamically reshape the privacy–personalization relationship. Second, studies employ heterogeneous outcomes attitudes, intentions, disclosure, avoidance, clicking, and purchasing making their conclusions difficult to compare. Third, empirical research remains dominated by cross-sectional surveys, self-reported intentions, single platforms, and Western samples; consequently, actual behavior and emerging-market contexts are underrepresented. Fourth, technological and regulatory changes have outpaced cumulative theory. AI-based inference, cross-platform profiling, opaque data brokerage, and privacy-enhancing advertising require an updated synthesis extending beyond cookie-based behavioral targeting. Although AI may create efficient and convenient consumer experiences, its opacity can weaken autonomy and trust unless appropriate human agency is retained (Puntoni et al., 2021).

This systematic literature review aims to identify, classify, and synthesize research published during the last decade on the relationships among data privacy, consumer trust, and digital-ad personalization. Specifically, it seeks to: (1) map the dominant theories, constructs, methods, and research contexts; (2) explain how privacy risks and personalization benefits influence consumer trust and behavioral responses; (3) identify the roles of transparency, control, data sensitivity, collection methods, platform context, and consumer characteristics; and (4) develop a research agenda applicable to contemporary algorithmic advertising. The proposed novelty lies in positioning consumer trust as the integrative mechanism connecting data-governance practices with the acceptance or rejection of personalized advertising. Instead of reducing the phenomenon to a binary privacy–benefit trade-off, the review combines privacy calculus, communication privacy management, psychological reactance, persuasion knowledge, and signaling theory. It consequently proposes a multilevel perspective linking organizational data practices, consumer cognitive–affective evaluations, contextual moderators, and behavioral outcomes.

In conclusion, personalized advertising becomes sustainable not when firms maximize the amount of consumer data processed, but when they establish a legitimate and trustworthy value exchange. Relevance without transparency may be interpreted as surveillance, while transparency without meaningful control may provide only symbolic assurance. A systematic integration of privacy and trust research is therefore necessary to explain the conditions under which personalization creates consumer value rather than resistance. Such synthesis can strengthen advertising theory while informing responsible, consumer-centered, and context-sensitive digital marketing practices.

METHODS

This study employed a systematic literature review (SLR) to synthesize conceptual and empirical evidence concerning the relationships among data privacy, consumer trust, and digital advertising personalization. An SLR was selected because it enables transparent, reproducible, and theory-oriented consolidation of a fragmented research domain (Snyder, 2019; Xiao & Watson, 2019). The review procedure followed the PRISMA 2020 reporting framework, particularly its requirements for documenting identification, screening, eligibility assessment, and final inclusion (Page et al., 2021). The analytical logic also followed the theory–context–characteristics–method approach recommended for developing a critical research agenda rather than producing a merely descriptive summary (Paul & Criado, 2020).

The literature search was conducted in Scopus and Web of Science because both databases provide broad coverage of peer-reviewed research in marketing, communication, information systems, and consumer behavior. Searches covered publications issued from January 2016 to September 2026. The search string combined the terms: (“data privacy” OR “privacy concern*” OR “privacy calculus”) AND (“consumer trust” OR “brand trust” OR “platform trust”) AND (“personalized advertising” OR “digital advertising” OR “online behavioral advertising” OR “ad personalization”). Backward and forward citation searches were subsequently performed to identify relevant studies omitted by the database query.

Articles were eligible when they: (1) were peer-reviewed journal articles written in English; (2) addressed consumer-facing digital or personalized advertising; (3) examined privacy and trust, or a theoretically proximate mechanism such as perceived vulnerability, transparency, control, or reactance; (4) reported an explicit conceptual framework and empirical findings; and (5) provided sufficient methodological information for evaluation. Conference papers, dissertations, books, non-peer-reviewed

reports, purely technical privacy studies, and articles unrelated to advertising personalization were excluded. Following duplicate removal, 148 titles and abstracts were screened. Forty full-text reports were assessed, and 30 were excluded because they fell outside the focal relationship, lacked empirical evidence, were not peer reviewed, or provided insufficient privacy/trust measures. The final analytical corpus comprised 10 articles.

The selected studies represented complementary theoretical and empirical perspectives. Martin et al. (2017) connected data vulnerability, transparency, and control with trust and firm performance, while Martin (2018) demonstrated the trust penalty produced by privacy violations. Kim et al. (2019) established that ad transparency is beneficial only when disclosed information flows are perceived as acceptable. Chen et al. (2019) explained consumer resistance through vulnerability and psychological reactance, whereas Strycharz et al. (2019) examined motivations to disable personalization. More recent evidence addressed the attention economy (Cloarec, 2020), the benefits and risks of behavioral advertising (Aiolfi et al., 2021), voluntary disclosure and privacy assurance (Zeng et al., 2021), privacy-boundary violations (Zhu & Kanjanamekanant, 2021), and consumer-brand relationships within privacy calculus (Hayes et al., 2022).

Data were extracted using a structured matrix containing authorship, year, country, platform, sample, theory, constructs, research design, principal findings, limitations, and proposed relationships. Methodological quality was assessed through construct clarity, sampling adequacy, analytical rigor, and correspondence between evidence and conclusions. The findings were synthesized thematically into four domains: perceived personalization benefits, privacy risks, trust-building mechanisms, and behavioral responses. Because the studies were heterogeneous in design and measurement, narrative synthesis was preferred to statistical meta-analysis. This procedure supported an integrative framework in which consumer trust links data-governance practices to the acceptance or rejection of personalized advertising.

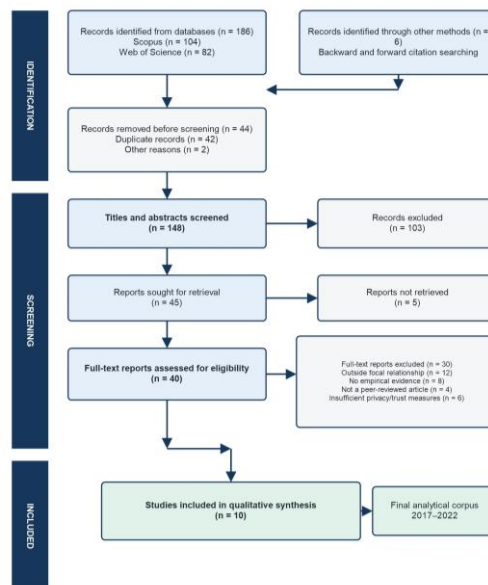


Figure 1. Prisma 2020 flow diagram

RESULTS AND DISCUSSION

Result

Characteristics of the Selected Studies

The systematic selection process generated a final corpus of 10 peer-reviewed articles published between 2017 and 2022. The corpus demonstrates a multidisciplinary structure: the studies were situated in marketing, advertising, information management, consumer behavior, and cyberpsychology. Experimental and survey designs predominated, although the evidence also included a field experiment, computational behavior tracking, an event study, and multistudy research. This methodological variation strengthens the synthesis because the focal relationships were observed through stated perceptions, experimentally manipulated data practices, actual protective behavior, purchasing responses, and organizational performance.

Table 1. Conceptual and empirical profile of the reviewed articles

Study	Context and empirical design	Main conceptual lens/ constructs	Principal empirical result
Martin et al. (2017)	Three-study design involving experiments, a security-breach event study of 414 public firms, and customers of 15 firms	Data vulnerability, perceived violation, transparency, control, and trust	Access to personal data increased feelings of violation and reduced trust. Transparency and consumer control mitigated these negative effects. Security breaches harmed firm performance and produced spillover effects.
Martin (2018)	Factorial-vignette surveys involving 845 participants across four samples and 33,800 vignette evaluations	Privacy as a social contract; ability, benevolence, integrity, and trust	Violating privacy expectations directly reduced website trust and weakened the impact of conventional trust-repair cues. Selling data to aggregators and targeting consumers' contacts were especially damaging.
Kim et al. (2019)	Six laboratory and field studies examining advertising-transparency disclosures	Information-flow norms, privacy-personalization trade-off, and platform trust	Transparency reduced advertising effectiveness when it revealed unacceptable data flows, particularly inferred or cross-platform information. It improved performance when data flows were acceptable and platform trust was high.
Chen et al. (2019)	Consumer survey analyzed using a rational-choice model	Psychological reactance, ownership, vulnerability, privacy concern, and opportunity cost	Feelings of ownership and vulnerability shaped consumers' cost-risk assessments. Privacy concerns and perceived opportunity costs increased reactance toward personalized advertising.
Strycharz et al. (2019)	Online experiment ($N = 425$) and online behavior tracking ($N = 80$)	Protection motivation theory, technical knowledge, and threat and coping appraisal	Technical knowledge did not automatically empower users. It could indirectly reduce opt-out motivation, whereas protection motivation was strongly associated with actual opt-out behavior.
Aiolfi et al. (2021)	Italian online survey using a visual online behavioral advertising (OBA) stimulus ($N = 128$); PLS-SEM	Perceived benefits, privacy concern, acceptance, avoidance, clicks, and purchase responses	Informativeness and entertainment supported OBA acceptance, whereas privacy concerns promoted avoidance. Acceptance and avoidance had distinct downstream effects on clicking and purchasing.
Zeng et al. (2021)	Large-scale, two-stage field experiment using propensity-score matching and difference-in-differences	Foot-in-the-door effect, self-disclosure, privacy assurance, and personalization declaration	Voluntary disclosure and greater disclosure intensity increased purchase responses to personalized promotions. Privacy assurance combined with an explicit personalization declaration encouraged disclosure.
Zhu and Kanjanamekanant (2021)	Online-market survey of Facebook users in Taiwan ($N = 349$)	Communication privacy management, information and social boundaries,	Internal data sources, perceived personification, and platform co-ownership improved perceived privacy, advertising attitudes, and

		and perceived privacy	purchase intentions. Boundary-incongruent data use produced resistance.
Morimoto (2021)	Comparative survey across social-media platforms in Japan	Persuasion knowledge, information control, privacy concern, and advertising evaluation	Persuasion knowledge increased privacy concern, while perceived information control conditioned this relationship. Privacy responses differed across Twitter, Facebook, and Instagram.
Hayes et al. (2022)	National 2 × 2 × 2 experiment examining relationship strength, overt/covert collection, and Facebook/Twitter	Privacy calculus, consumer-brand relationship, and perceived benefits and risks	Strong consumer-brand relationships increased perceived benefits and mitigated disclosure risks. In weaker relationships, perceived risk dominated the privacy calculus.

Conceptual Synthesis

Four conceptual clusters emerged from the coding. First, privacy calculus explains personalized advertising as a conditional exchange. Consumers may tolerate data collection when relevance, convenience, information quality, or economic value outweigh anticipated privacy costs. This mechanism is supported by Aiolfi et al. (2021), Zeng et al. (2021), and Hayes et al. (2022). However, the calculus is relational rather than purely economic: prior brand relationships and platform trust determine whether the same data practice is interpreted as beneficial or exploitative.

Second, privacy-boundary congruence determines the legitimacy of personalization. Kim et al. (2019) and Zhu and Kanjanamekanant (2021) consistently indicate that data obtained within the focal platform, voluntarily supplied by consumers, or used within an expected relationship is more acceptable than inferred, sensitive, externally acquired, or third-party data. Thus, privacy is not equivalent to complete data secrecy; it concerns whether information flows correspond with contextual expectations and perceived ownership.

Third, trust functions as a mediating and buffering mechanism. Martin et al. (2017) demonstrate that data vulnerability affects outcomes through perceived violation and trust, while Martin (2018) shows that privacy violations can damage both trust levels and the effectiveness of traditional trust cues. Kim et al. (2019) and Hayes et al. (2022) further establish that pre-existing platform or brand trust can expand the zone in which personalization is considered acceptable. Trust, however, cannot legitimize every practice: it amplifies the benefit of norm-consistent transparency but cannot fully compensate for boundary violations.

Fourth, consumer agency converts privacy evaluation into behavior. Chen et al. (2019) identify reactance as a response to threatened autonomy, whereas Strycharz et al. (2019) demonstrate that knowledge alone does not guarantee protective action. Morimoto (2021) similarly shows that information control changes how persuasion knowledge is translated into privacy concern. These findings distinguish nominal transparency from effective empowerment: consumers require intelligible explanations, usable controls, and realistic opportunities to refuse personalization.

Cross-Study Empirical Patterns

The thematic coding found privacy risk or vulnerability in all 10 studies. Five studies directly identified transparency, assurance, or control as a mitigating condition; four explicitly positioned trust or relationship strength as a mechanism; and four documented reactance, avoidance, or opt-out responses. Positive personalization outcomes appeared principally when three conditions coincided: the benefit was recognizable, the data flow was contextually appropriate, and the consumer retained meaningful agency. Negative outcomes occurred when personalization made surveillance salient, disclosed unexpected inference or sharing, or signaled that information had been processed without authorization.

The synthesis therefore rejects a universal linear relationship in which greater personalization automatically produces stronger advertising outcomes. Instead, the evidence supports a conditional trust pathway:

Responsible data practice → perceived transparency and control → lower privacy risk and higher trust
→ acceptance, engagement, and purchase response.

An opposing pathway was equally visible:

Opaque or boundary-incongruent data use → perceived vulnerability or violation → trust erosion and psychological reactance → avoidance, opt-out, and weaker purchase response.

Integrated Finding

The central result of this review is that consumer trust constitutes the principal conversion mechanism between data privacy practices and the effectiveness of personalized digital advertising. Personalization creates value only when its informational benefits exceed privacy costs within a relationship perceived as legitimate. Transparency is therefore effective when it explains acceptable practices, control is effective when it permits consequential choice, and personalization is effective when it remains proportionate to the sensitivity and origin of the data. Collectively, the evidence indicates that privacy-respectful personalization is not merely an ethical constraint but a prerequisite for sustainable advertising performance.

Discussion

Personalization as a Conditional Value Exchange

The synthesis demonstrates that digital advertising personalization does not produce uniformly positive or negative consumer responses. Its effectiveness is conditional on how consumers evaluate the value obtained from personalization relative to the privacy costs created by data collection, inference, and sharing. This finding supports privacy calculus theory, according to which disclosure and acceptance depend on a comparison between anticipated benefits and perceived risks. However, the reviewed evidence extends a purely economic interpretation of that calculus. Consumers do not merely calculate whether a relevant advertisement is worth surrendering data; they also evaluate whether the underlying information flow is legitimate, whether the advertiser is trustworthy, and whether they retain meaningful control over the exchange. Empirically, Aiolfi et al. (2021) show that informativeness and entertainment can promote acceptance of online behavioral advertising, whereas privacy concerns stimulate avoidance. Zeng et al. (2021) similarly demonstrate that self-disclosure can increase purchase responses when it is preceded by privacy assurance and an explicit declaration of personalization. Hayes et al. (2022) add a relational dimension: a strong consumer–brand relationship increases perceived benefits and mitigates disclosure risks, while risk dominates when that relationship is weak. Thus, the value of personalization is not inherent in algorithmic accuracy. It is socially constructed through the perceived fairness, relevance, and legitimacy of the data exchange. This interpretation is consistent with Bol et al. (2018), who found that benefits, privacy costs, and trust jointly predict disclosure across personalized media contexts. The privacy paradox should therefore not be interpreted as consumer indifference. Privacy concerns are related to protective behavior, but the concern–behavior relationship is constrained by knowledge, resources, habits, and interface conditions (Baruh et al., 2017; Gerber et al., 2018). Continued platform use may reflect dependence or limited alternatives rather than genuine consent.

Consumer Trust as the Central Explanatory Mechanism

The primary theoretical contribution of the findings is the positioning of consumer trust as the mechanism that converts data-governance practices into advertising outcomes. Trust represents a willingness to accept vulnerability based on positive expectations regarding an organization's ability, integrity, and benevolence. Within personalized advertising, this vulnerability is substantive because consumers cannot directly observe how algorithms combine, infer, store, or transfer their information. Martin et al. (2017) provide strong evidence that merely granting a firm access to personal data can heighten perceived violation and reduce trust. Their findings further show that transparency and control suppress these adverse effects, while security breaches create both consumer-level and firm-performance penalties. Martin (2018) extends this conclusion by showing that privacy violations create a double penalty: they reduce trust directly and weaken the influence of conventional trust cues. Once a company has violated information-flow expectations, claims of competence or benevolence become less persuasive. Trust is consequently cumulative but fragile; it can widen consumers' tolerance for responsible personalization, yet it deteriorates rapidly when corporate behavior contradicts stated privacy commitments. Trust also explains heterogeneity in advertising effectiveness. Kim et al. (2019) found that transparency about acceptable information flows can improve advertising responses on trusted platforms, whereas transparency exposing unacceptable flows makes privacy concerns more salient and reduces effectiveness. Hayes et al. (2022) similarly show that strong brand relationships alter privacy calculus by strengthening benefits and lowering perceived disclosure risk. Indonesian evidence points in the same direction: perceived data transparency strengthens the positive relationship between personalization and consumer trust, whereas privacy concern

weakens trust through poorer transparency evaluations (Hidayat et al., 2025). Collectively, these findings indicate that trust is neither a static antecedent nor a simple outcome. It operates as a recursive resource: responsible data use builds trust, trust facilitates acceptance, and accepted interactions can reinforce the relationship; violations reverse this cycle.

Contextual Integrity and the Boundaries of Acceptable Personalization

The results further reveal that privacy judgments depend on contextual integrity rather than the absolute quantity of collected information. Consumers assess who obtained the data, where it originated, what type of information was used, and whether its use corresponds with the original context. Kim et al. (2019) show that voluntarily stated and within-platform information is generally perceived as more acceptable than inferred or cross-platform data. Zhu and Kanjanamekanant (2021) likewise find that internal data sources, perceived personification, and platform co-ownership improve perceived privacy, advertising attitudes, and purchase intentions. This distinction clarifies why highly relevant advertising can feel either helpful or “creepy.” Relevance based on an explicit product search remains intelligible within a commercial exchange, while an advertisement revealing inferred health conditions, private conversations, or cross-device surveillance violates the expected informational boundary. Boerman et al. (2017) conceptualize online behavioral advertising as an interaction between advertiser-controlled factors such as personalization level and transparency and consumer-controlled factors, including knowledge, perceptions, and individual characteristics. The current synthesis refines that framework by identifying boundary congruence as the point at which these factors converge. Personalization becomes acceptable when consumers understand why an advertisement appears and regard the data source and purpose as proportionate.

Transparency, Control, and the Limits of Formal Consent

Transparency and control emerge as necessary but insufficient conditions for trustworthy personalization. A disclosure can increase trust only when it is understandable, timely, specific, and connected to a consequential choice. Kim et al. (2019) demonstrate that transparency may backfire when it reveals objectionable practices. Accordingly, firms should not treat disclosure as a cosmetic instrument for legitimizing unrestricted tracking. Transparency does not transform an inappropriate data flow into an acceptable one; it merely makes the practice more visible. The same qualification applies to consumer control. Morimoto (2021) found that information control conditions the relationship between persuasion knowledge and privacy concern across social-media platforms. Strycharz et al. (2019), however, show that technical knowledge alone does not necessarily empower consumers and may even indirectly reduce opt-out motivation. This apparently counterintuitive result suggests that awareness must be paired with self-efficacy and usable mechanisms. Consumers who understand tracking but face complex settings, repeated consent requests, or take-it-or-leave-it choices may develop resignation rather than agency. These results distinguish substantive control from procedural consent. Substantive control enables consumers to access, limit, or withdraw processing, whereas procedural consent merely records agreement. Boerman and Smit (2023) similarly identify privacy cynicism as a research priority. The managerial objective should therefore be to improve the quality of authorization, not merely maximize consent rates.

Psychological Reactance and Defensive Consumer Responses

Where consumers perceive surveillance or a loss of autonomy, privacy evaluation becomes behavioral resistance. Chen et al. (2019) demonstrate that feelings of ownership and vulnerability influence privacy concerns and perceived opportunity costs, which subsequently increase reactance. Reactance is theoretically important because it explains why technically relevant advertisements may be rejected: resistance is directed not only toward message content but also toward the perceived restriction of freedom embedded in the targeting process. The reviewed studies reveal several defensive outcomes, including advertisement avoidance, opt-out behavior, reduced clicking, negative attitudes, and weaker purchase intention. Strycharz et al. (2019) find a strong relationship between protection motivation and actual opt-out behavior, while Aiolfi et al. (2021) show that privacy concerns encourage OBA avoidance. Zhu and Kanjanamekanant (2021) demonstrate that perceived privacy improves both advertising attitude and purchase intention, implying that privacy protection contributes directly to performance rather than merely preventing harm. These results challenge the assumption that more granular targeting necessarily improves conversion. Excessive personalization can increase short-term relevance while damaging long-term trust, platform attitudes, and customer equity.

Cross-Platform and Consumer Heterogeneity

The privacy–trust relationship is also context dependent. Morimoto (2021) reports different evaluations across Twitter, Facebook, and Instagram, while Hayes et al. (2022) show that platform and

relationship conditions jointly shape privacy calculus. Consumers may tolerate recommendations in e-commerce yet reject equivalent inference on a platform associated with interpersonal communication. Privacy literacy, prior experience, relationship strength, vulnerability, and trust propensity further influence whether data use appears useful or intrusive. Gerber et al. (2018) therefore caution against assuming a universal privacy paradox. Future research should use configurational and longitudinal designs to identify conditions producing trust, resignation, or resistance.

Theoretical and Managerial Implications

Conceptually, the review integrates privacy calculus, contextual integrity, psychological reactance, communication privacy management, and trust theory into two competing pathways. In the value-creation pathway, appropriate data collection, intelligible transparency, and meaningful control reduce perceived risk and build trust, enabling relevance to improve engagement and purchase responses. In the vulnerability pathway, opaque collection, sensitive inference, or unauthorized sharing produces perceived violation, trust erosion, reactance, and avoidance. Trust is the switching mechanism between these pathways. For managers, the findings imply that responsible personalization should be designed around data minimization, first-party data, purpose limitation, proportionality, and consumer-accessible controls. Advertisers should explain why an advertisement is shown, identify the categories of data used, distinguish stated from inferred information, and allow consumers to modify or reject targeting. Performance evaluation should extend beyond clicks to include trust, complaints, opt-out rates, perceived fairness, and long-term relationship quality. The literature therefore supports a strategic conclusion: privacy protection is not external to advertising effectiveness. It is an organizational capability that preserves the legitimacy of personalization. Overall, the evidence resolves the apparent conflict between privacy and personalization by showing that consumers do not categorically reject data-driven relevance. They reject personalization that lacks contextual legitimacy, proportionality, or meaningful agency. Trust allows consumers to accept unavoidable uncertainty, but it cannot permanently compensate for intrusive practices. Sustainable personalized advertising consequently requires a shift from maximizing data extraction toward maximizing justified relevance. Firms that treat privacy as a relationship-quality mechanism rather than a compliance burden are more likely to secure both consumer acceptance and durable advertising performance.

CONCLUSION

This systematic literature review synthesized 10 peer-reviewed studies published between 2017 and 2022 to explain how data privacy and consumer trust shape responses to personalized digital advertising. Conceptually, the evidence integrates privacy calculus, communication privacy management, psychological reactance, contextual integrity, and trust theory. The resulting framework positions consumer trust as the central mechanism connecting organizational data practices with advertising acceptance or resistance. Personalization is therefore not inherently beneficial or intrusive; its consequences depend on the legitimacy of data collection, the sensitivity and origin of information, transparency, consumer control, platform context, and relationship strength. Empirically, the reviewed studies consistently show that relevant and informative personalization can improve advertising attitudes, engagement, self-disclosure, and purchase responses. These positive effects occur primarily when data are voluntarily provided, collected within an expected context, and supported by credible privacy assurances. Conversely, covert tracking, third-party sharing, sensitive inference, and privacy violations increase perceived vulnerability, reduce trust, stimulate psychological reactance, and encourage avoidance or opt-out behavior. Transparency is beneficial only when it reveals acceptable information flows, while technical knowledge without usable control does not necessarily empower consumers. Accordingly, sustainable personalized advertising requires data minimization, intelligible disclosure, meaningful consent, and accessible preference controls. Privacy protection should be treated not merely as regulatory compliance but as a strategic capability for preserving trust and long-term advertising effectiveness.

REFERENCES

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: Benefits and risks of online behavioral advertising. *International Journal of Retail & Distribution Management*, 49(7), 1089–1110. <https://doi.org/10.1108/IJRDM-10-2020-0410>

- 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>
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. <https://doi.org/10.1111/jcom.12276>
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of Advertising*, 46(3), 363–376. <https://doi.org/10.1080/00913367.2017.1339368>
- Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: An overview of past research and a research agenda. *International Journal of Advertising*, 42(1), 60–68. <https://doi.org/10.1080/02650487.2022.2122251>
- Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, 23(6), 370–388. <https://doi.org/10.1093/jcmc/zmy020>
- Chen, Q., Feng, Y., Liu, L., & Tian, X. (2019). Understanding consumers' reactance of online personalized advertising: A new scheme of rational choice from a perspective of negative effects. *International Journal of Information Management*, 44, 53–64. <https://doi.org/10.1016/j.ijinfomgt.2018.09.001>
- Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, 161, 120299. <https://doi.org/10.1016/j.techfore.2020.120299>
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226–261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2022). The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing*, 55, 16–30. <https://doi.org/10.1016/j.intmar.2021.01.001>
- Hidayat, A. S., Mardani, A. D., & Pramulanto, H. (2025). Personalization vs. privacy: Balancing data-driven marketing and consumer trust in the digital economy. *YUME: Journal of Management*, 8(1), 1191–1201. <https://doi.org/10.37531/yum.v8i1.9010>
- Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, 45(5), 906–932. <https://doi.org/10.1093/jcr/ucy039>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, 82, 103–116. <https://doi.org/10.1016/j.jbusres.2017.08.034>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58. <https://doi.org/10.1509/jm.15.0497>
- Morimoto, M. (2021). Privacy concerns about personalized advertising across multiple social media platforms in Japan: The relationship with information control and persuasion knowledge. *International Journal of Advertising*, 40(3), 431–451. <https://doi.org/10.1080/02650487.2020.1796322>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372*, Article n71. <https://doi.org/10.1136/bmj.n71>

- Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *International Business Review, 29*(4), Article 101717. <https://doi.org/10.1016/j.ibusrev.2020.101717>
- Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. Journal of Marketing, 85(1), 131–151. <https://doi.org/10.1177/0022242920953847>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13(2), Article 1. <https://doi.org/10.5817/CP2019-2-1>
- Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. Journal of Planning Education and Research, 39(1), 93–112. <https://doi.org/10.1177/0739456X17723971>
- Zarouali, B., Poels, K., Ponnet, K., & Walrave, M. (2018). “Everything under control?": Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 12(1), Article 5. <https://doi.org/10.5817/CP2018-1-5>
- Zeng, F., Ye, Q., Li, J., & Yang, Z. (2021). Does self-disclosure matter? A dynamic two-stage perspective for the personalization–privacy paradox. Journal of Business Research, 124, 667–675. <https://doi.org/10.1016/j.jbusres.2020.02.006>
- Zhu, Y.-Q., & Kanjanamekanant, K. (2021). No trespassing: Exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media. Information & Management, 58(2), 103314. <https://doi.org/10.1016/j.im.2020.103314>