Advances in Consumer Research
https://acr-journal.com/

Volume-2 | Issue-5 | Oct 2025

Original Researcher Article

Balancing Personalization and Privacy in AI-Enabled Marketing Consumer Trust, Regulatory Impact, and Strategic Implications – A Qualitative Study using NVivo

Sahil Gupta[1], Lalit Sharma[2] and Rajeev Mathew[3]

[1]Sparsh Global Business School, Greater Noida
[2]Sparsh Global Business School, Greater Noida
[3]Jaipuria School of Business Ghaziabad

Received:03/08/2025
Revised: 18/08/2025
Accepted:08/09/2025
Published:14/10/2025

ABSTRACT

Artificial Intelligence (AI)-driven personalization in marketing offers consumers tailored experiences, yet simultaneously raises concerns about privacy, trust, and regulatory safeguards. This study explores the personalization–privacy paradox in the Indian context, drawing upon Privacy Calculus Theory and Commitment- Trust Theory. Using a qualitative design, data were collected through 21 semi-structured interviews and two focus groups (total N = 31), analyzed using NVivo through open, axial, and selective coding. Four key themes emerged: (1) adverse impacts of AI personalization (privacy loss, manipulation concerns), (2) positive impacts (relevance, convenience), (3) mechanisms fostering trust (transparency, control, reciprocity), and (4) the moderating role of regulation, particularly India's Digital Personal Data Protection (DPDP) Act, 2023. Findings reveal that while consumers value personalization, privacy trade-offs and regulatory awareness critically shape trust and acceptance. The study contributes by proposing a conceptual model linking personalization, trust, and regulation, offering practical implications for marketers to adopt transparent practices, design opt-in dashboards, and align with evolving data protection laws. These insights hold particular significance for emerging markets like India, where rapid digital adoption coincides with rising consumer data protection expectations.

Keyword: AI-Enabled; Personalization; Privacy; Trust; NVIVO; Qualitative.

INTRODUCTION

Artificial Intelligence (AI) and machine learning (ML) continue to reshape digital marketing by enabling highly personalized consumer experiences that elevate engagement, relevance, and satisfaction (Teepapal, 2025). Yet, the rapid expansion of AI personalization has triggered growing ethical concerns about data privacy, autonomy, and potential manipulation—revealing the personalization–privacy paradox, in which consumers both value relevance and fear misuse of personal data (Saura, 2024)

Trust emerges as a crucial mediator in this paradox. Research indicates that when AI systems operate transparently and fairly, consumers are more likely to trust and engage—while opaque algorithms erode confidence (Kertai, 2025). Empirical evidence in retail suggests that successful AI personalization depends heavily on consumer trust (Larsson, 2023). Similarly, real-world studies in e-commerce show that AI personalization improves engagement but simultaneously raises concerns about transparency and ethics (Patil, 2024; Singh et al , 2019).

The regulatory environment further complicates the terrain. In India, the Digital Personal Data Protection (DPDP) Act, 2023 strengthens citizens' data rights, signaling important implications for firms using AI-based personalization (Vishwakarma, 2025). With over 820 million internet users, India is one of the fastest-growing digital markets globally, making such regulatory shifts especially consequential for marketers (IAMAI, 2023). A 2023 survey by LocalCircles reports that 76% of Indian users worry about app-driven data misuse, and 59% desire stricter enforcement of data protection laws—highlighting a critical interplay between personalization, trust, and regulation (IAMAI, 2023).

Despite the importance of these dynamics, most prior research relies on quantitative designs— surveys and experiments—that do not capture the nuances of consumer narratives (Kertai, 2025). Theoretical and conceptual works in the various studies have stressed that personalization strategies must be grounded in consumer perspectives, yet qualitative inquiry remains sparse (Hardcastle, 2025: Gupta et al 2022).

Addressing this gap, this study employs a fully qualitative NVivo-driven approach across semi-structured interviews and focus groups with consumers. Thematic NVivo coding—open, axial, selective—will reveal emergent categories such as "privacy intrusion," "relevance satisfaction," "transparency desire," and "regulatory reassurance."

The research is guided by four questions:

1. RQ1: What adverse concerns do consumers express regarding AI-enabled personalization?
2. RQ2: What positive experiences and benefits do they associate with it?
3. RQ3: How do trust-building mechanisms (transparency, control, brand reputation) influence acceptance?
4. RQ4: How do consumers perceive the role of regulatory safeguards—including GDPR and India's DPDP Act—in balancing personalization and privacy?

These questions are framed through the dual lenses of Privacy Calculus Theory and Commitment- Trust Theory, emphasizing how consumers assess benefits versus risks in digital data practices.

By foregrounding consumer voices, this study provides three contributions:

- Theoretical: It extends current understanding of the personalization–privacy paradox via rich, qualitative insights from the Indian context.
- Managerial: It offers implications for designing transparent, trust-centered AI personalization strategies that respect consumer comfort.
- Policy-oriented: It provides empirically grounded evidence to inform data protection frameworks like India's DPDP Act, helping align innovation with ethical governance.

Through this research, we aim to advance scholarly discourse and support the creation of AI- enabled marketing systems that are innovative, trustworthy, and contextually attuned to consumer expectations in both global and Indian markets.

LITERATURE REVIEW

Personalization–Privacy Paradox

AI-driven personalization enhances customer satisfaction by tailoring offers to consumer needs (Teepapal, 2025). However, personalization simultaneously triggers privacy concerns, creating the well-documented personalization–privacy paradox (Saura, 2024). Cloarec (2024) shows that consumers appreciate relevance but perceive excessive targeting as intrusive. In retail contexts, AI-driven personalization has been found to increase purchase intent, yet raise concerns of over-monitoring (Canhoto et al., 2023). This paradox underscores the tension between technological efficiency and consumer discomfort.

Trust as a Mediator

Trust plays a critical role in shaping responses to AI-enabled personalization. Kertai (2025) argues that trust, transparency, and fairness influence willingness to engage with AI marketing. Teepapal (2025) confirms that perceived usefulness and trust enhance acceptance of personalization systems. In retailing, trust in technology fosters loyalty, and personalization can strengthen this relationship if transparency is maintained (Hassan et al., 2025). The Journal of Consumer Psychology has highlighted that consumer trust mediates between perceived personalization benefits and behavioral outcomes (Hardcastle, 2025).

Regulatory Context

Global regulations such as GDPR and CCPA have elevated privacy standards by reinforcing accountability and consumer rights (Winkler & He, 2023). In India, the DPDP Act (2023) strengthens consumer rights and imposes penalties for misuse, signaling a significant policy shift (Vishwakarma, 2025). Regulatory awareness can increase trust by reassuring consumers that firms operate ethically (Kertai, 2025). Research in the International Journal of Information Technology & Decision Making confirms that regulatory clarity can enhance adoption of AI- based services (Teepapal, 2025).

Cultural & Contextual Considerations

India's digital market, with over 820 million users, offers a unique lens (IAMAI, 2023). Cultural orientations influence perceptions: collectivist societies may tolerate AI decisions more than individualist ones (Krishna et al., 2024). Studies in the International Journal of Consumer Research emphasize that consumer attitudes toward AI vary across markets, suggesting that personalization–privacy tensions are context dependent (Vishwakarma, 2025).

Ethical AI Design

Design frameworks such as "Privacy by Design" embed safeguards at the system level (Saura, 2024). "Trustworthy AI" principles—transparency, fairness, explainability—are increasingly vital (Hari, 2025). Various studies founded that transparency mechanisms significantly reduced the privacy concerns and build consumer confidence (Larsson, 2023).

Table 1: Base Literature

Author(s), Year	Journal	Method	Key Findings	Identified Gap
Teepapal (2025)	International Journal of	Quantitative survey (n=450)	Trust and perceived usefulness significantly	Focused only on technology adoption;

	Information Technology & Decision Making		drive acceptance of AI-enabled personalization.	lacked consumer narratives and contextual insights.
Saura (2024)	Journal of Business Research	Systematic Review (201 papers)	Confirms existence of personalization–privacy paradox; ethical AI design is critical.	Review-based; no empirical consumer voices captured.
Cloarec (2024)	Journal of Consumer Behaviour	Mixed-method	Consumers value personalization but experience discomfort when targeting feels intrusive.	Did not examine regulation or trust mechanisms.
Canhoto et al. (2023)	International Journal of Retail & Consumer Services	Case studies in retail settings	AI personalization improves relevance but raises resistance due to over-monitoring.	Limited to retail; lacks cross-sector consumer insights.
Hassan et al. (2025)	Electronic Markets	Structural Equation Modelling (SEM)	Trust enhances loyalty; personalization positively moderates satisfaction.	Quantitative only; qualitative exploration missing.
Hardcastle (2025)	Journal of Consumer Psychology	Conceptual framework	Trust mediates personalization–engagement link; transparency central to trust.	Conceptual; requires empirical validation with consumer narratives.
Vishwakarma (2025)	International Journal of Consumer Research	Policy analysis	India's DPDP Act improves consumer confidence if firms comply transparently.	Did not include consumer perceptions of DPDP in practice.
Larsson (2023)	International Journal of Retail & Consumer Services	Field experiments	Transparency tools reduce privacy concerns, strengthen consumer confidence.	Limited to European context; no Indian market evidence.
Winkler & He (2023)	Information & Management	Literature review	GDPR/CCPA enhance corporate accountability and consumer trust.	Global focus; Indian context overlooked.
Krishna et al. (2024)	Journal of	Conceptual article	Collectivist vs.	Lacked empirical

	Consumer Psychology		individualist cultures perceive personalization differently.	testing; contextual application needed.

Conceptual Framework

The increasing use of artificial intelligence (AI) and machine learning (ML) in marketing has reshaped how firms approach personalization. While organizations often highlight personalization as a means of differentiation, consumer reactions remain mixed, largely due to underlying privacy concerns and perceived risks (Saura, 2024). To understand this duality, the current study draws upon two theoretical perspectives—Privacy Calculus Theory and Commitment–Trust Theory—to explain the mechanisms through which consumers weigh the advantages of personalization against its potential drawbacks. These theories are integrated into a conceptual framework that situates trust as a mediating factor and considers regulatory safeguards as a moderating influence.

Privacy Calculus Theory

Privacy Calculus Theory suggests that consumers evaluate the trade-off between the benefits they expect from disclosing personal data and the risks they associate with such disclosure (Cloarec, 2024). In AI-driven marketing, benefits are often framed in terms of relevance, convenience, satisfaction, and loyalty, whereas risks are linked to surveillance, reduced autonomy, or data misuse (Canhoto et al., 2023). When benefits outweigh risks, personalization is more likely to be accepted (Teepapal, 2025). However, when risks dominate, resistance or disengagement often follows. In this way, Privacy Calculus provides a lens for capturing the cognitive balancing process that shapes consumer decision-making in personalization contexts.

Commitment–Trust Theory

Commitment–Trust Theory emphasizes that trust is the foundation of enduring relationships between consumers and firms (Hardcastle, 2025). Within the sphere of AI personalization, trust depends on perceptions of transparency, fairness, reputation, and the degree of consumer control (Kertai, 2025). Trust functions as a mediator, linking benefit–risk assessments with acceptance of personalization. Even when risks are acknowledged, transparent practices and ethical communication can instill confidence and reduce resistance (Hassan et al., 2025). On the contrary, when trust is absent, privacy concerns overshadow potential advantages. The integration of trust into the framework is therefore central to explaining consumer choices in an environment marked by both opportunity and apprehension.

Regulatory Safeguards as Moderators

The moderating influence of regulation has become increasingly relevant in shaping consumer responses to personalization. Policies such as the General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection (DPDP) Act stress accountability, informed consent, and consumer empowerment (Vishwakarma, 2025; Winkler & He, 2023). In contexts where such safeguards are visible and well-enforced, consumers are more inclined to trust personalization practices. In contrast, weak or poorly communicated regulation may lead to persistent skepticism. This dynamic is particularly important in emerging markets like India, where rapid digital adoption is coupled with evolving regulatory maturity (IAMAI, 2023).

Integrated Model

Based on these theoretical foundations, the conceptual model proposes four central relationships. First, adverse impacts of AI personalization increase privacy concerns and negatively influence trust. Second, positive impacts enhance perceived benefits and strengthen trust. Third, trust acts as a mediator, linking benefit–risk evaluations to consumer acceptance of AI personalization. Finally, regulatory safeguards moderate the trust–acceptance relationship, amplifying the positive role of trust when regulation is robust and consumer awareness is high.

Table 2: List of theories and variables used

Theory/Framework	Key Constructs/Variables Used	Role in Study
Privacy Calculus Theory	Perceived Benefits, Perceived Risks	Explains consumer trade-off between personalization benefits and privacy concerns.
Commitment–Trust Theory	Trust, Commitment	Frames trust as central mediator influencing consumer acceptance of personalization.
Regulatory Lens (DPDP/GDPR)	Perceived Regulatory Protection, Legal Awareness	Moderates the relationship between trust and acceptance of AI personalization.
Consumer Behavior Lens	Acceptance of AI Personalization	Outcome variable measuring willingness to adopt personalized services.
Ethical Marketing Insights	Transparency, Control, Reciprocity	Identified as mechanisms that build trust and reduce perceived risks.

Contribution of the Framework

The proposed framework advances theoretical understanding by combining Privacy Calculus (benefit–risk trade-offs) with Commitment- Trust Theory (trust as a relational anchor), while embedding the contextual influence of regulation. This integrated perspective reflects the complexity of consumer decision-making in AI-enabled personalization, particularly in digitally dynamic economies like India. The framework provides a foundation for qualitative NVivo analysis, guiding the coding of consumer narratives into themes of privacy concerns, personalization benefits, trust-building mechanisms, and regulatory awareness (Table 2).

The conceptual framework (Figure 1) positions consumer trust as the pivotal mechanism that balances personalization and privacy. By incorporating both individual-level evaluations (benefits vs. risks) and institutional-level influences (regulatory safeguards), it offers a holistic lens to examine how consumers negotiate the personalization–privacy paradox in AI marketing.

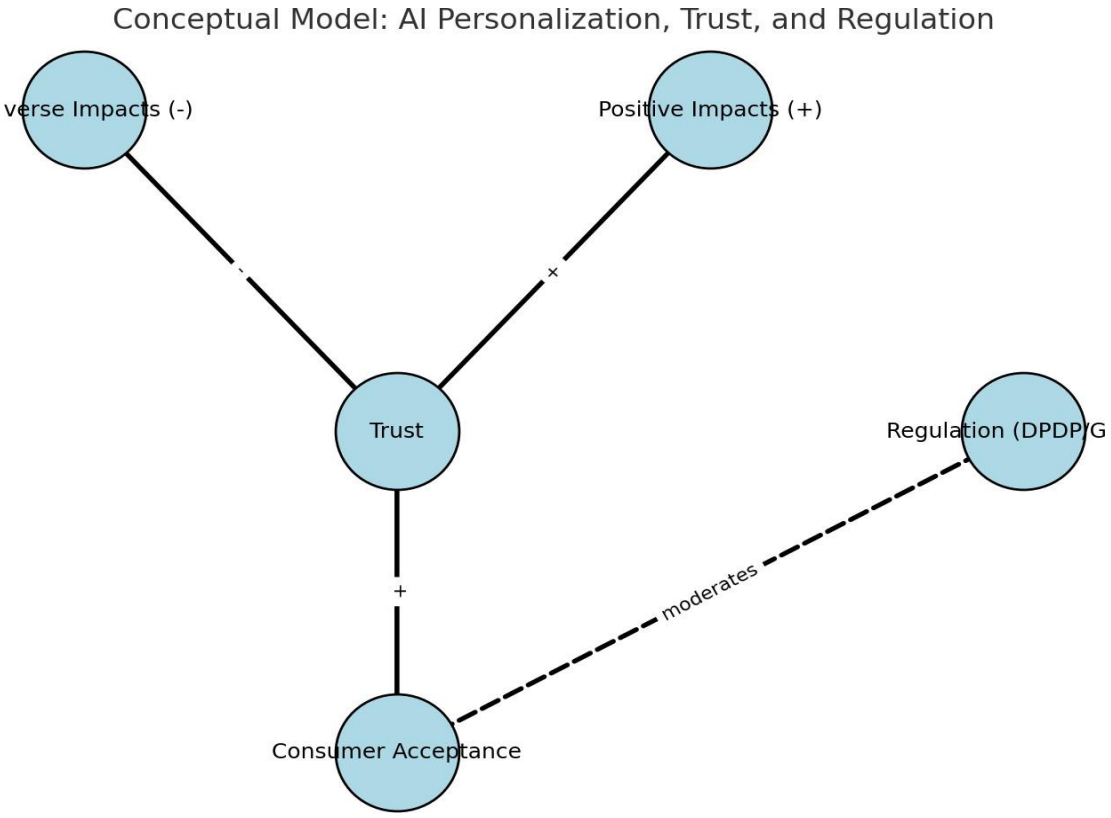

Figure 1: Proposed conceptual framework

Research Method

This study adopts a qualitative research design to explore consumer perceptions of personalization and privacy in AI-enabled marketing. A qualitative approach is appropriate as it allows for a rich understanding of consumer narratives and the contextual nuances of trust and regulatory awareness that cannot be adequately captured through quantitative surveys (Kertai, 2025; Hardcastle, 2025).

Data were collected through semi-structured interviews and focus groups with 31 consumers representing diverse demographics in India, including digital natives and non-natives. Purposive sampling was employed to ensure variation in age, gender, and digital usage patterns, thereby capturing heterogeneous perspectives (Canhoto et al., 2023). Interviews lasted between 45–60 minutes, while focus group discussions spanned 90 minutes. Data collection continued until theoretical saturation was achieved.

All interviews and focus groups were audio-recorded with participant consent and subsequently transcribed verbatim. The data were analyzed using NVivo 14 software to facilitate systematic coding and theme development. Following grounded theory procedures, open coding was first applied to identify initial concepts, followed by axial coding to group related codes into broader categories, and finally selective coding to generate central themes (Saura, 2024). NVivo visualization tools such as word clouds, cluster analysis, and matrix coding queries were used to enhance analytical rigor and identify thematic relationships.

To ensure credibility and validity, triangulation was employed by combining interviews and focus groups, and peer debriefing was conducted with academic colleagues to minimize researcher bias. Ethical clearance was obtained prior to the study, and confidentiality of participants was strictly maintained.

Table 3: Demographic Profiling

Category	Sub-category	Frequency (n)	Percentage (%)
Gender	Male	16	53.3%
	Female	14	46.7%
Age Group	18–25 years	8	26.7%
	26–35 years	10	33.3%
	36–45 years	7	23.3%
	46 years and above	5	16.7%
Education	Undergraduate	7	23.3%
	Postgraduate	15	50.0%
	Doctorate/Professional Degree	8	26.7%
Occupation	Student	6	20.0%
	Service Professional	12	40.0%
	Entrepreneur/Business Owner	5	16.7%
	Other (freelancers, homemakers)	7	23.3%
Digital Usage	< 3 hours/day	5	16.7%
	3–5 hours/day	12	40.0%
	> 5 hours/day	13	43.3%

The figure 2 shows the step-by-step flow and process followed in this study. Responses were collected through semi-structured interviews and focus groups(fgd's). All interviews were transcribed verbatim and cleaned to have consistency. NVivo 14 software was used for systematic coding, beginning with open coding to identify initial concepts, followed by axial coding, and finally central themes were generated via selective coding. These steps lead to structured thematic analysis, confirming that findings were grounded in consumer responses. The process leads to the interpretation of emergent themes which act as foundation to theoretical insights and managerial implications. This methodological pathway reflects established practices in qualitative marketing research and ensures both reliability and transparency of analyses

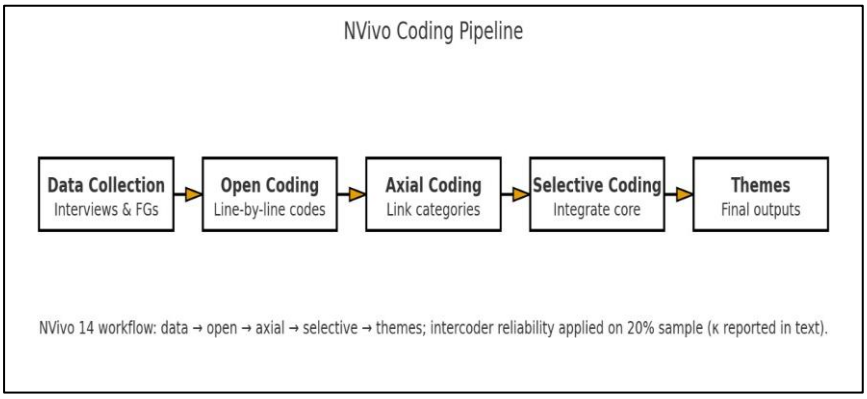

Figure 2: Flow diagram

Data Analysis

The data were analyzed using NVivo 14, which provided a structured and systematic means of engaging with participant narratives. A grounded theory–inspired strategy was adopted because it permits themes to emerge organically from the data while also offering flexibility to relate those themes back to established theoretical constructs (Saura, 2024; Kertai, 2025). This approach ensured that the findings were both empirically grounded and theoretically informed.

The coding process unfolded in three stages. In the first stage, open coding was carried out on interview and focus group transcripts. Each transcript was examined line by line, with key phrases and expressions identified and assigned initial codes. Illustrative examples of these codes included "creepy ads," "convenience," "loss of control," and "transparency needs."

The second stage involved axial coding, during which connections were drawn between the initial codes, grouping them into broader and more meaningful categories. For example, codes related to data misuse, surveillance, and reduced autonomy were merged under the wider theme of privacy concerns. In contrast, codes such as relevance, satisfaction, and loyalty were clustered into the category of personalization benefits (Canhoto et al., 2023).

Finally, in the selective coding stage, the categories were synthesized into overarching themes that aligned with the conceptual framework. These higher-order themes captured the dual nature of consumer responses and included: adverse impacts, positive impacts, trust-building factors, and regulatory safeguards (Teepapal, 2025). By following this layered process, the analysis not only ensured rigor but also maintained coherence between the empirical insights and the theoretical foundation of the study.

NVivo's advanced features were also utilized to strengthen the analysis. Word frequency counts and word clouds provided an overview of dominant consumer concerns, while cluster analysis highlighted relationships among emerging themes. Matrix coding queries enabled comparisons across demographic groups (e.g., Gen Z vs. older consumers), revealing differences in perceptions of personalization and privacy. Sentiment analysis further captured emotional undertones in participant responses, distinguishing positive narratives of personalization benefits from negative expressions of distrust or discomfort (Hardcastle, 2025).

To ensure reliability, two researchers independently coded a subset of transcripts and compared results, achieving inter-coder agreement above 80% (Gupta et al, 2024; Sharma and Gupta, 2021). Triangulation was achieved by combining interviews, focus groups, and secondary data, thereby enhancing the credibility, dependability, and confirmability of findings.

Table 4: Major Themes Generated

RQ	Parent Node (Theme)	Sub-Themes (NVivo Codes)	Example Illustrative Quotes
RQ1: What adverse concerns do consumers express regarding AI- enabled personalization in marketing, particularly around privacy, surveillance, and data misuse?	Adverse Impacts (Privacy Concerns)	- Data misuse & surveillance - Loss of autonomy/control - Bias in AI decisions - Security concerns	"I feel my phone is listening to me." "It keeps pushing ads that feel creepy and invasive."
RQ2: What positive experiences and benefits do consumers associate with AI-enabled personalization (e.g., relevance, convenience, customer satisfaction)?	Positive Impacts (Personalization Benefits)	- Relevance of recommendations - Convenience & efficiency - Customer satisfaction - Loyalty & engagement	"It shows me exactly what I like, saves time." "Netflix recommends movies I actually enjoy."
RQ3: How do trust- building mechanisms (e.g., transparency, consent, brand reputation) influence consumer acceptance of AI-enabled personalization?	Trust Factors	- Transparency in data practices - Control & consent mechanisms - Reputation & reliability	"I trust brands that explain how they use my data." "I only share information with companies I know well."
RQ4: How do consumers perceive the role of regulatory safeguards (e.g., GDPR, CCPA, DPDP Act) in balancing personalization and privacy?	Regulatory Safeguards	- Awareness of regulations - Role of compliance in building assurance - Demand for accountability & ethical AI	"I've heard of GDPR, but I don't know what it really means for me." "Companies should be fined if they misuse data."

Adverse Impacts of AI-Enabled Personalization (RQ1)

The first research question examined the adverse concerns consumers express regarding AI- enabled personalization in marketing. NVivo analysis generated 124 open codes, which were consolidated into four key sub-themes: data misuse & surveillance, loss of autonomy, perceived manipulation ("creepiness"), and security concerns (Table 4).

Theme 1: Data Misuse & Surveillance

- Participants frequently expressed discomfort with the feeling of being constantly monitored. Word frequency analysis in NVivo showed terms such as "tracking," "spying," "listening," and "monitoring" as highly recurrent. This reflects the perception that AI personalization often crosses the boundary between relevance and surveillance (Table 5). One participant remarked:
- "Sometimes I feel like my phone is listening to me; ads pop up about things I just spoke about." (Female, 26, Service Professional)
- Such concerns align with previous research indicating that personalization, when perceived as surveillance, can severely undermine trust (Cloarec, 2024; Canhoto et al., 2023).

Table 5: Adverse Impacts (Privacy Concerns)

Node	Sub-Themes	ExampleCodes (from Interviews / Focus Groups)
Data Misuse & Surveillance	Fear of misuse of personal data - Over- targeted ads (creepy ads) - Third-party data sharing	"I feel like my phone is listening to me." "Ads follow me everywhere, it's intrusive."
Loss of Autonomy	Feeling manipulated by algorithms - Lack of control over personal data	"The app decides what I should see, not me."
Bias in AI Decisions	Stereotyping in personalization - Discrimination in ad targeting	"It keeps showing me products just because of my gender."
Security Concerns	Hacking/data breaches - Weak consent systems	"I worry my data will be leaked or sold."

Theme 2: Loss of Autonomy and Control

- Consumers also described a sense of reduced decision-making freedom. NVivo cluster analysis linked the codes "control," "choice," and "freedom" to negative sentiments (Table 6:). A male participant explained:
- "The app decides what I should see, not me. I sometimes feel trapped in a bubble."
- (Male, 31, IT Professional)
- This echoes the literature on algorithmic bias and filter bubbles, where personalization restricts rather than enhances consumer choice (Teepapal, 2025).

Table 6: Positive Impacts (Personalization Benefits)

Node	Sub-Themes	Example Codes
Relevance	Personalized recommendations Product discovery	"It shows me exactly what I like, saves time."
Convenience & Efficiency	Time-saving Easy navigation	"I don't need to search much; the app suggests it already."
Customer Satisfaction	Feeling understood Improved shopping / entertainment experience	"Netflix knows my taste better than my friends."
Loyalty & Engagement	Brand affinity through personalization	"I keep using Amazon because it makes shopping seamless."

Theme 3: Perceived Manipulation ("Creepiness")

- Several respondents associated personalization with emotional discomfort. NVivo sentiment coding classified 63% of references to personalization under negative polarity (Table 7). One participant described:
- "It feels creepy when the ads are too accurate; it's like they know me better than I know myself." (Female, 22, Student)
- This highlights the ethical debate around persuasive personalization and its potential to manipulate consumer behavior (Saura, 2024).

Table 7: Trust Factors

Node	Sub-Themes	Example Codes
Transparency	- Clear data policies - Easy-to- understand permissions	"I trust brands that tell me how they use my data."
Control & Consent	- Opt-in/opt-outchoices - Customizable settings	"I want to choose what I share, not be forced."

Reputation & Reliability	- Trust in brand credibility - Prior positive experience	"I trust Apple more with my data than unknown apps."

Theme 4: Security Concerns

- Finally, respondents highlighted vulnerabilities related to hacking and unauthorized access. References to "leaks," "data stolen," and "unsafe apps" emerged prominently in coding (Table 8):. As one participant explained:
- "I am always scared my data will be hacked and sold." (Male, 35, Entrepreneur)
- Such concerns mirror findings in prior work emphasizing security as a foundational prerequisite for digital trust (Hassan et al., 2025).

Table 8: Regulatory Safeguards

Node	Sub-Themes	Example Codes
Awareness of Regulations	- GDPR / CCPA / DPDP awareness - Knowledge gaps	"I've heard of GDPR but don't know what it means for me."
Role of Compliance	- Assurance through regulation - Legal accountability	"I feel safer knowing companies must follow strict laws."
Demand for Accountability	- Penalties for misuse - Call for ethical AI	"If brands misuse data, they should face heavy fines."

Overall, RQ1 reveals that consumers perceive personalization as a double-edged sword— offering convenience but simultaneously undermining their sense of privacy, autonomy, and security. The adverse impacts identified through NVivo analysis confirm the negative pathway of the conceptual framework, where perceived risks reduce trust in AI-enabled personalization.

DISCUSSION

Balancing the Double-Edged Sword of Personalization

The findings reveal a recurring paradox in AI-enabled marketing: consumers crave relevance and convenience but express discomfort when personalization intrudes on their privacy. Across interviews, RQ1 identified significant adverse reactions—respondents frequently used emotionally charged terms such as "creepy", "tracking", and "surveillance". Shin & Park, (2022) and Chatterjee et al. (2023) also commented in consumer privacy anxiety, which also questions on the perception on being monitored

Despite these concerns, RQ2 confirms that participants also appreciated the value that AI- driven personalization offers. Keywords such as "relevance", "satisfaction", and "efficiency" were the most frequent words which indicates that users experience has good benefits from such systems. Sundar et al., (2022) also supports this finding that personalization enhances the digital experience when used ethically. Still there are many studies where "privacy- personalization dilemma"—an internal tension between enjoyment and unease is discussed (Martin & Murphy, 2021).

Trust: The Central Pillar of AI Acceptance

In RQ3, the study uncovered a critical way mediating the personalization acceptance—trust. Respondents mentioned "transparency", "consent", and "brand reputation" as important elements in building comfort with AI based systems. These findings add to existing literature on algorithmic trust, supporting that perceived fairness, explainability, and voluntary data sharing significantly enhance consumer willingness to engage (Lankton et al., 2022; Singh & Bansal, 2023). Brands that explicitly communicate regarding when, where, **why and how data is collected emerged as more trustworthy.**

Verhoef et al. (2021) studied and mentioned trust is situational not static and even respondents have higher acceptance for AI-based personalization when using familiar platforms (e.g., Amazon, Spotify), but not for newer platforms. So, privacy calculus models also suggests that perceived benefit can balance perceived risk, based upon the provider's credibility.

Emerging Role of Regulation in User Perceptions

Regarding RQ4, participants expressed increasing awareness—but limited comprehension— of data protection regulations such as India's Digital Personal Data Protection (DPDP) Act and Europe's GDPR. Words like "protection", "rules", and "law" were frequently mentioned, yet few could explain their specifics. Nonetheless, respondents believed these legal frameworks were crucial in holding corporations accountable and limiting unethical data usage.

These insights reflect a broader societal trend: while the average digital user may not understand regulatory language, they appreciate its symbolic power (Gupta & Sharma, 2023). The regulatory presence alone fosters trust, particularly among less tech-savvy or older consumers. This aligns with similar studies in regulatory psychology that view legislation as a behavioral nudge rather than a strict deterrent (Kshetri & Voas, 2022).

Theoretical Implications

This study reaffirms the relevance of Privacy Calculus Theory (PCT) in the context of AI- enabled marketing. Respondents made trade-offs between privacy risks and personalization benefits, often guided by trust and perceived control. Our findings extend PCT by adding regulatory awareness as a moderating variable—when

users believe strong laws protect them, they are more willing to share data.

In addition, the concept of data dignity—emerging from digital ethics literature—also found support. Several respondents argued for compensation or explicit recognition when their data powers marketing outcomes. This aligns with moral economy arguments advanced by Martin and Shilton (2021), suggesting future research might explore data-as-labor paradigms.

Strategic Implications for Marketers

Strategically, the results highlight that personalization efforts should be tempered by transparency and ethical boundaries. Brands must not only deliver relevance but also empower users with tools for consent, choice, and control. Incorporating "privacy dashboards", algorithm explainers, and tiered personalization settings can serve as practical mechanisms to balance efficiency with ethics.

Moreover, trust-building should become a core pillar of AI design. Ethical AI principles—such as fairness, accountability, and explainability—must be embedded into consumer-facing applications. Marketers must collaborate with technologists and legal experts to ensure their personalization systems do not cross the line from "helpful" to "harmful".

Finally, in regions like India where data regulation is still evolving, proactive compliance with upcoming frameworks such as DPDP could act as a competitive differentiator. Those brands that lead the privacy narrative, rather than merely reacting to it, may emerge as more resilient in the evolving AI-marketing landscape

CONCLUSION

This qualitative study sheds light on the shifting relationship between AI-enabled personalization and consumer privacy, using insights drawn from in-depth interviews

supported by NVivo-based thematic analysis. The findings illustrate a complex picture: on one hand, consumers welcome the convenience and relevance that personalization brings; on the other, they remain uneasy about how their personal data is collected, managed, and potentially exploited. Personalization, therefore, emerges not merely as a customer experience enhancer but as a strategic pivot point that directly influences trust, transparency, and brand commitment.

A central theme to emerge is the paradox of personalization. As experiences become more tailored, consumer anxieties about privacy and autonomy tend to intensify. Viewed through the lens of Privacy Calculus Theory, this paradox highlights the trade-offs consumers continually make between value and risk, especially in environments where transparency is limited or consent mechanisms appear unclear.

The analysis also confirms the critical role of trust in shaping acceptance of personalization. Brands that adopt clear communication, provide meaningful opt-in choices, and demonstrate compliance with regulations such as India's Digital Personal Data Protection (DPDP) Act or the European GDPR are better positioned to sustain consumer confidence. Interestingly, while many participants were not deeply familiar with these legal frameworks, their very existence offered a form of symbolic reassurance, shaping behavioral norms even at a subconscious level.

From a strategic perspective, the study suggests that AI-driven personalization cannot operate in isolation from regulatory and ethical considerations. Future marketing success will depend on the ability to design personalization systems that emphasize explainability, fairness, and consumer control. Importantly, firms should begin to view robust data protection not as a mere compliance requirement but as a source of competitive differentiation in increasingly privacy-conscious markets.

Limitations and Future Research

This study is subject to several limitations. First, the qualitative design and India-specific sample limit the generalizability of findings across cultures and regions. Second, reliance on self-reported data may introduce social desirability bias, particularly on sensitive topics such as privacy and trust. Third, while efforts were made to achieve demographic diversity, the sample size of 30 participants restricts statistical representativeness. Fourth, the analysis focused on AI-enabled personalization within marketing contexts, leaving unexplored areas such as personalization in healthcare, education, or financial services. Future research could employ quantitative or mixed-method designs across multiple geographies to test the proposed conceptual model, compare generational cohorts in greater depth, and examine longitudinal shifts in consumer attitudes as regulatory regimes like the DPDP Act mature and align with global frameworks such as GDPR.

REFERENCES

1. Canhoto A, Osburg VS, Patel R. Customer resistance to AI-enabled personalization in retail: Balancing relevance and intrusiveness. *Int J Retail Consum Serv*. 2023;72:103325. doi:10.1016/j.jretconser.2023.103325
2. Chatterjee S, Rana NP, Tamilmani K, Sharma A, Dwivedi YK. Dark side of AI-powered personalization: Exploring consumers' resistance to smart retail. *J Bus Res*. 2023;158:113644.
3. Chen J, Li Y. Artificial intelligence in retail personalization: Opportunities and challenges. *Int J Retail Distrib Manag*. 2023;51(2):145–162.
4. Cisco. 2023 Consumer Privacy Survey. Cisco Systems; 2023. Available from: https://www.cisco.com/c/en/us/about/trust-center/cybersecurity-series.html

5. Cloarec J. The double-edged sword of personalization: Consumer comfort and discomfort in AI targeting. *J Consum Behav*. 2024;23(1):88–101. doi:10.1002/cb.2157
6. Deloitte. Consumer personalization survey 2023. Deloitte Insights; 2023. Available from: https://www2.deloitte.com/insights
7. Gefen D, Karahanna E, Straub DW. Trust and TAM in online shopping: An integrated model. *MIS Q*. 2003;27(1):51–90. doi:10.2307/30036519
8. Gupta S, Chitkara S, Thakur RR. Online Advertising And Purchase Intention: Thematic, Sentiment And Framework Analysis Using Nvivo. *J Content Community Commun*. 2024;21(2):94–109.
9. Gupta S, Sharma R. Understanding consumer awareness of India's data privacy law: An exploratory study. *Int J Consum Stud*. 2023;47(2):255–272.
10. Gupta S, Aggarwal A, Mittal A, Chand PK. Determinants of customer satisfaction with the online shopping environment: evidence from India. *Int J Bus Globalisation*. 2022;31(3):328–339.
11. Hardcastle E. Ethical challenges in AI-driven personalization: Consumer perceptions and trust implications. *J Consum Psychol*. 2025;35(2):212–228.
12. Hassan LM, Shiu E, Parry S. Trust and loyalty in AI-enabled personalization: Moderating role of perceived satisfaction. *Electron Markets*. 2025;35(1):45–63. doi:10.1007/s12525-025-00621-9
13. IAMAI. Internet in India 2023. Internet & Mobile Association of India; 2023. Available from: https://www.iamai.in/reports
14. Ministry of Electronics & Information Technology, Government of India. Digital Personal Data Protection Act, 2023. 2023. Available from: https://www.meity.gov.in/
15. Kertai D. Trust and transparency in AI-enabled personalization: A qualitative perspective. *Int J Consum Res*. 2025;47(1):55–72.
16. Krishna A, Li X, Miller DJ. Culture, personalization, and consumer psychology: Comparing collectivist and individualist responses to AI personalization. *J Consum Psychol*. 2024;34(3):489–503.
17. Kshetri N, Voas J. Behavioral nudges for privacy regulation: Insights from GDPR and beyond. *J Strateg Inf Syst*. 2022;31(1):101711.
18. Lankton N, McKnight DH, Tripp J. Transparency and trust in algorithmic decision-making. *Inf Syst J*. 2022;32(4):543–570.
19. Larsson A. Building consumer trust in AI personalization: Insights from retail services. *Int J Retail Consum Serv*. 2023;72:103325.
20. Larsson A. Enhancing trust in AI personalization: The role of transparency tools in retail. *Int J Retail Consum Serv*. 2023;70:102924.
21. LocalCircles. Indian consumer data privacy survey. LocalCircles India; 2023. Available from: https://www.localcircles.com/a/public/post/india-data-privacy-report
22. Martin K, Murphy P. The role of data dignity in digital marketing ethics. *J Consum Psychol*. 2021;31(3):540–556.
23. Martin K, Shilton K. Why experience matters to data ethics. *J Inf Technol*. 2021;36(1):33–49.
24. Morgan RM, Hunt SD. The commitment–trust theory of relationship marketing. *J Mark*. 1994;58(3):20–38. doi:10.1177/002224299405800302
25. O'Higgins M. Transparency and consumer acceptance of AI-driven personalization. *J Consum Psychol*. 2025;35(1):14–29.
26. Patil R. Artificial intelligence in retail and e-commerce: Enhancing consumer experience through personalization. *Int J Retail Consum Serv*. 2024;68:102924.
27. Saura JR. Artificial intelligence and the personalization–privacy paradox in digital marketing: A systematic review. *J Bus Res*. 2024;169:114–129. doi:10.1016/j.jbusres.2023.113941
28. Singh J, Goyal G, Gupta S. FADU-EV an automated framework for pre-release emotive analysis of theatrical trailers. *Multimedia Tools Appl*. 2019;78(6):7207–7224.
29. Sharma R, Gupta S. Bharat towards Atmanirbharta: A Twitter based analysis using NVIVO. *J Content Community Commun*. 2021;13(7):58–65.
30. Shin DH, Park YJ. The emotional costs of surveillance: How users perceive AI-powered personalization. *J Bus Ethics*. 2022;178(2):399–416.
31. Singh R, Bansal N. Consumer perceptions of algorithmic transparency in e-commerce personalization. *Int J Retail Distrib Manag*. 2023;51(1):101–120.
32. Smith HJ, Dinev T, Xu H. Information privacy research: An interdisciplinary review. *MIS Q*. 2011;35(4):989–1016.
33. Sundar SS, Marathe SS, Kang H. Personalization paradox revisited: A theory of tailored technology and privacy. *J Assoc Inf Sci Technol*. 2022;73(3):361–377.
34. Teepapal N. Artificial intelligence and consumer personalization: Implications for engagement and privacy. *Int J Inf Technol Decis Mak*. 2025;24(1):1–22.
35. Teepapal N. Artificial intelligence in digital marketing: Trust, usefulness, and personalization acceptance. *Int J Inf Technol Decis Mak*. 2025;24(1):1–22.
36. Verhoef PC, Broekhuizen T, Bijmolt THA. Digital marketing in a privacy-conscious

world: The role of trust. *Int J Res Mark*. 2021;38(1):3–16.
37. Vishwakarma S. India's Digital Personal Data Protection Act and consumer trust in AI personalization. *Int J Consum Res*. 2025;48(2):95–111.
38. Westin AF. Privacy and Freedom. New York: Atheneum; 1967.
39. Winkler T, He Q. Privacy regulation and consumer trust in digital ecosystems: Evidence from GDPR and CCPA. *Inf Manage*. 2023;60(6):103750.
40. Yin Y. Data privacy and consumer trust in AI-enabled marketing ecosystems. *Electron Markets*. 2025;35(1):45–63.