

AI-Powered Personalization vs. Consumer Privacy: Striking the Balance in Indian Digital Marketing

Hardik Beniwal¹, Pooja Khanna² and Rajeev Kaur³

¹Research Scholar,

Email: hardikbeniwal74@gmail.com

²Professor, Department of English, Aditi Mahavidyalaya, University of Delhi.

Email: poojak@aditi.du.ac.in

³Professor, Department of Commerce, Aditi Mahavidyalaya, University of Delhi.

Email: rajeevkaur@gmail.com

Received: 26/12/2024

Revised: 30/12/2024

Accepted: 07/01/2025

Published: 30/01/2025

ABSTRACT

In a world where artificial intelligence quietly shapes everything from what we buy to how we think, Indian consumers are increasingly being pulled into a web of hyper-personalized digital experiences. But behind the seamless recommendations and tailored ads lies a growing concern: what is the real cost of convenience? This study explores how Indian consumers make sense of AI-driven personalization in digital marketing, and how their expectations, discomforts, and trust are shaped by it. Through in-depth, semi-structured interviews with consumers across different regions and age groups, we uncover a rich set of emotions, ranging from fascination to fear. While many participants appreciate the ease and relevance AI offers, there's a persistent unease about where their data goes, who's watching, and whether consent is ever truly informed. The findings reveal a strong gap between how personalization is experienced and how privacy is understood. Most consumers trade personal data for convenience without fully grasping the implications, an imbalance that's made worse by confusing privacy policies and a lack of transparency from platforms. India's recently enacted Digital Personal Data Protection (DPDP) Act, 2023, although a step in the right direction, remains largely invisible in everyday consumer awareness. This research calls for a more thoughtful approach, one where businesses prioritize transparency, design AI tools with built-in respect for privacy, and regulators step in not just with laws, but with public literacy campaigns. Striking the balance between personalization and privacy isn't just a technical or legal challenge, it's a human one.

Keywords: Artificial Intelligence (AI), Digital Marketing, Personalization, Consumer Privacy, Data Protection, Qualitative Research.



© 2025 by the authors; licensee Advances in Consumer Research. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY-NC-ND) license (<http://creativecommons.org/licenses/by/4.0/>).

INTRODUCTION

"The more we know about you, the better we can serve you."

A mantra echoed by modern marketers, but at what cost?

From customized Spotify playlists to eerily accurate shopping suggestions on Flipkart, personalization is no longer a luxury, it's the expectation. In India's rapidly digitizing economy, artificial intelligence has become the invisible architect of our online experiences. Every click, swipe, and scroll feeds algorithms designed to anticipate what we want before we ask. To many consumers, this feels like convenience. To others, it feels like surveillance dressed as service.

As Indian businesses embrace AI to build deeper, data-driven relationships with their customers, they're also walking a thin line between personalization and privacy. While the tech promises relevance, speed, and efficiency, it often leaves users wondering: What did I consent to? Who has my data? Can I really trust the apps I use every day?

This tension isn't just technical, it's deeply human. It touches on trust, autonomy, identity, and the right to be forgotten in a world that remembers everything.

In this study, we explore how Indian consumers perceive AI-powered personalization in digital marketing, and what privacy means to them in a cultural context where data is often shared without a second thought. Through qualitative interviews and

thematic analysis, we aim to uncover the stories, anxieties, trade-offs, and hopes that shape the Indian digital consumer's experience.

Because striking a balance isn't just about better policies or smarter algorithms, it's about listening to people first.

Framing the Tension: Navigating AI Personalization and Consumer Privacy in the Indian Digital Landscape
In this qualitative inquiry, we explore the growing dilemma faced by Indian consumers and marketers alike: how to embrace the convenience of AI-powered personalization without compromising individual privacy. While artificial intelligence offers relevance and speed in digital marketing, it simultaneously raises deep ethical questions about consent, transparency, and data control, especially in a culturally diverse and digitally evolving market like India.

This study aims to uncover how consumers in India perceive AI personalization, what privacy-related anxieties they face, and how digital marketers negotiate this delicate trade-off. It also evaluates the role of India's Digital Personal Data Protection Act (2023) in safeguarding user rights. Using semi-structured interviews and document analysis, the research foregrounds lived experiences rather than abstract metrics, making space for real voices in a conversation often dominated by algorithms and policy papers.

By bridging academic theory and real-world insight, this study holds value not only for scholars but also for businesses, policymakers, and AI practitioners seeking to build ethical and culturally aware digital systems in the Indian context.

LITERATURE REVIEW

Artificial intelligence (AI) has become a key driver in the evolution of digital marketing, reshaping how brands communicate, sell, and build relationships with consumers. Through technologies such as chatbots, recommendation engines, predictive modelling, and behavioural tracking, AI enables marketers to tailor experiences in real-time. In India, platforms like Flipkart, Zomato, Swiggy, Paytm, and Cred exemplify the rise of hyper-personalized marketing, delivering offers, suggestions, and content based on users' digital behaviour. Flipkart leverages deep learning to customize product feeds (Kumar & Sinha, 2022), while Zomato refines restaurant suggestions based on past orders. Swiggy uses geo-targeted personalization and dynamic pricing (Nanda & Pathak, 2021), and Paytm applies AI to credit scoring and financial personalization (Saxena, 2023). Cred tailors gamified reward systems based on lifestyle and spending behaviour (Sharma & Iyer, 2024).

While the marketing benefits of AI are evident, personalization of this scale raises serious ethical and privacy concerns. In digital environments, privacy is not just a technical issue but a psychological and cultural one. Westin (1967) defined privacy as the

ability to control how personal information is shared, yet this notion becomes complex in societies like India, where digital literacy is uneven and social norms vary across regions. Indian consumers frequently exhibit contradictory behaviour, valuing convenience while being uneasy about surveillance, what scholars describe as the "privacy paradox" (Norberg et al., 2007). Many users engage with personalized platforms while remaining unaware of how their data is collected, stored, or monetized (Mitra & Rathi, 2022). This lack of awareness often leads to "consent fatigue," where users accept terms without reading or understanding them. Compounded by complex privacy policies and opaque data practices, consent becomes more symbolic than meaningful (Raj & Singh, 2023). Zuboff's (2019) concept of "surveillance capitalism" is highly relevant here, where user data becomes a commodity, feeding algorithms that shape not only what users see but what they want. In India, such dynamics are intensified by limited regulatory enforcement, language barriers, and social normalization of data sharing.

To address these issues, the Indian government introduced the Digital Personal Data Protection (DPDP) Act, 2023, which provides rights such as access, correction, and erasure of personal data, and emphasizes informed consent (Mehta, 2023). The Act introduces the notion of "Data Fiduciaries," placing legal responsibility on organizations that collect and process personal data. However, critics argue the law lacks teeth in enforcement, especially given broad government exemptions and weak penalties (Dutta, 2023). Compared to the European Union's GDPR, the DPDP Act appears more flexible but less rigorous. The GDPR mandates stronger consent mechanisms, cross-border data transfer restrictions, and significantly higher fines (Goyal & Fernandes, 2024). Moreover, while GDPR compliance is often visible on global platforms, the DPDP Act remains largely unfamiliar to the average Indian consumer.

Previous studies have explored consumer perspectives on AI and privacy, but qualitative insights from the Indian context remain limited. Araujo et al. (2020) found that in the UK, personalization is accepted when it feels contextual and earned, but triggers discomfort when it crosses into perceived manipulation. In India, Hari and Bibiyana (2024) explored AI-driven marketing in Chennai, revealing a generational divide: younger consumers tended to embrace personalization, while older users expressed feelings of intrusion. Sayyed et al. (2025), in their study of hyper-personalization in the banking sector, reported themes of trust, risk perception, and data control. Farooq et al. (2025) noted that while Indian consumers appreciated AI recommendations, most had little understood of how these systems worked or what data was being collected.

Despite these valuable insights, several gaps remain in the literature. Few studies examine perspectives from semi-urban or rural areas, where mobile internet

penetration is growing rapidly. There is also limited exploration of how gender, language, and socio-economic status influence privacy concerns. In a market as diverse as India, consumer experiences with AI personalization are shaped by more than just technology, they are deeply tied to cultural values, economic realities, and power dynamics between users and platforms.

This study addresses these gaps by adopting a qualitative approach to foreground the voices of Indian consumers. It focuses on their lived experiences, trust dynamics, expectations, and the emotional and cognitive trade-offs they make when navigating AI-driven digital ecosystems. The aim is not only to understand how personalization is perceived, but also to reflect on how privacy is understood, negotiated, or overlooked in everyday digital interactions.

METHODOLOGY

This study adopts a qualitative, exploratory, and interpretive research design to investigate how Indian consumers perceive AI-driven personalization in digital marketing, and how they interpret the associated privacy implications. Rooted in the constructivist and phenomenological paradigms, the research seeks to understand the lived experiences of individuals, acknowledging that meaning is shaped through personal, cultural, and contextual lenses rather than objective measurements. Data were collected primarily through semi-structured interviews, allowing participants to express their views freely while the researcher-maintained consistency across key themes. The interviews were conducted with two main participant groups: digital consumers from diverse demographic backgrounds (urban, semi-urban, and different age groups), and digital marketing professionals from Indian companies that actively use AI personalization tools. This dual perspective offers a more holistic view of both the user experience and the marketing intent behind personalization practices. To supplement these interviews, document analysis was also conducted. This included a close reading of corporate privacy policies, marketing communication materials, and legal texts such as the Digital Personal Data Protection (DPDP) Act, 2023, to contextualize and compare stakeholder narratives with formal regulations.

All ethical considerations were carefully observed. Participants provided informed consent, and interviews were conducted in accordance with guidelines ensuring anonymity and confidentiality. Data were securely stored in encrypted digital formats, accessible only to the researcher. Care was taken to ensure that no personally identifiable information was disclosed in the final report. By adhering to these ethical standards, the study aims to uphold the trust and integrity essential to qualitative inquiry, especially when addressing topics as sensitive as data privacy and digital surveillance.

Findings

The findings of this study are drawn from in-depth, semi-structured interviews conducted with Indian digital consumers and marketing professionals, supported by document analysis of corporate privacy communications and legal texts. The data reveal a nuanced and often conflicted relationship between users and AI-driven personalization in digital marketing. Six key themes emerged from the thematic analysis, highlighting the emotional, social, and cognitive dimensions of consumer experience in India's AI-mediated digital ecosystem.

One of the most prominent themes was the value consumers placed on personalization. Many participants expressed appreciation for the convenience and relevance AI-enabled systems brought to their daily lives. Personalized ads, product suggestions, and content recommendations were often described as “helpful” or “time-saving,” particularly when aligned with shopping preferences, location, or browsing history.

“Sometimes I feel like the app knows me better than I know myself, it shows me things I didn’t even realize I needed,” said Priya (28), a working professional from Bengaluru.

This perceived utility appeared to reduce friction in decision-making and created a sense of being “understood” by digital platforms.

However, this convenience was accompanied by a deep ambiguity and fear around data usage. Participants frequently voiced discomfort about being monitored, profiled, or targeted without their knowledge. While some were aware that their actions online contributed to personalization, few could articulate how their data was collected, stored, or processed.

“I know they’re tracking me, but I have no idea what data they actually keep, and for how long,” noted Ankit (35), a business analyst from Pune. There was a near-universal lack of familiarity with privacy policies, which were often described as “too long,” “confusing,” or “never read.”

“I just click ‘Agree’ because what else can you do? If you don’t, you can’t use the app,” said Meena (42), a homemaker from Hyderabad.

This led to feelings of helplessness, with several users admitting they had “no choice” but to accept terms and conditions.

Cultural and social factors further shaped consumer behaviour. For many younger participants, data sharing had become normalized, driven by peer influence, social media trends, and the promise of rewards or exclusive content.

“If you want those cashback offers or coupons, you have to give access. Everyone does it,” explained

Raghav (22), a college student in Delhi. In contrast, older participants expressed more caution, often informed by distrust or lack of exposure to technology. These generational differences extended to notions of privacy itself: while some saw it as a right, others viewed it as a negotiable part of digital participation.

“I didn’t grow up with all this. I don’t know what these companies do with our information, and that worries me,” shared Mrs. D’Souza (58), a retired teacher from Goa.

Another recurring theme was trust in platforms, which varied significantly across users. Some respondents reported more trust in Indian platforms, believing they were “closer to home” and therefore more accountable. “At least with Indian apps, if something goes wrong, I can understand the terms or call support,” said Vivek (31), a freelance designer from Ahmedabad. Others felt safer with global brands due to perceived technological sophistication and adherence to international standards. Regardless of platform origin, interface design, clarity of communication, and ease of navigation played a crucial role in influencing trust levels.

“If an app gives me control over what data it collects, I trust it more. It’s not just about the brand,” said Tanisha (27), a digital marketing professional from Mumbai.

The communication practices of companies emerged as a critical concern. Participants noted a stark gap between what companies claimed in their privacy policies and what users actually experienced. Marketing messages often highlighted AI-driven personalization as a benefit, but without adequate disclosure of how data was used behind the scenes.

“They say ‘your privacy is important’ in ads, but they never explain what that means. It feels fake,” said Aamir (29), an app developer from Lucknow. There was a general sentiment that companies “don’t really explain what happens to your data,” leading to skepticism and, in some cases, disengagement.

Finally, when asked about legal protections and the recently enacted Digital Personal Data Protection (DPDP) Act, 2023, most participants had either never heard of the law or misunderstood its scope.

“DPDP? I’ve never heard of that. Is it like GDPR?” asked Kavya (24), a postgraduate student in Chennai. The absence of visible, user-facing education campaigns meant that the Act had yet to enter the public consciousness. Nonetheless, there was a strong desire for better regulation and enforcement. “There should be rules that make companies tell us clearly what they’re doing with our data, and they should be punished if they lie,” asserted Mahesh (45), a small business owner in Jaipur.

Together, these themes reveal a layered and complex picture: consumers in India welcome the benefits of AI personalization but lack the tools, knowledge, and legal support to fully understand or control the privacy trade-offs they are making. This disconnect presents a significant challenge not only for regulators but also for companies seeking to build ethical and trustworthy digital experiences

DISCUSSION

The findings of this study reveal the layered complexity of how Indian consumers engage with AI-driven personalization in digital marketing, especially in relation to their understanding of privacy. These insights reflect broader theoretical frameworks while also shedding light on context-specific dynamics unique to the Indian digital environment.

At the heart of this discussion lies the Privacy Calculus Theory, which suggests that individuals weigh the perceived benefits of information disclosure against potential privacy risks (Culnan & Bies, 2003). This trade-off was evident in participants’ willingness to share personal data in exchange for convenience, relevance, and rewards, even when they were unsure of the data’s destination or use. The consumer trust framework further helps explain why some users continued engaging with platforms despite privacy concerns. Trust, in this context, was shaped not only by company reputation or country of origin but also by the clarity of design and the ease with which users could access privacy controls. Finally, the theory of surveillance capitalism (Zuboff, 2019) provides a critical lens for understanding the structural imbalance between platforms and users, where consumer behaviour becomes the raw material for monetization, often without transparent consent.

These theoretical ideas manifest in specific Indian cultural contexts. For instance, many younger users viewed data sharing as a normalized part of digital life, heavily influenced by peer networks and social validation. Meanwhile, older participants or those from less digitally literate backgrounds expressed a more cautious stance, often rooted in uncertainty or mistrust. This generational and regional diversity reflects how privacy perceptions are not just individual but shaped by socio-economic, linguistic, and educational factors, factors that remain underexplored in dominant Western privacy literature.

One of the most visible areas where the privacy–personalization tension intensifies is in retargeted advertising, particularly when consumers see ads for products they only casually browsed. Several participants expressed unease over “being followed” by ads, perceiving it as intrusive. Voice assistants like Google Assistant or Alexa were also viewed with suspicion, with users concerned that these devices might be “listening all the time.” These examples point to a pressing need for ethical design principles, interfaces that foreground transparency, consent, and choice rather than default opt-ins. User

empowerment through accessible privacy settings, real-time notifications, and the ability to toggle personalization should become industry standards, not optional extras.

For marketers, the study offers clear implications. AI personalization, while effective, must be transparent in its operation. Companies need to move beyond legalistic privacy policies and adopt plain-language communication that explains what data is collected, how it is used, and why it matters. More importantly, customizable personalization settings, where users can actively shape the kind of content they want, can serve as a bridge between trust and technology. This will not only enhance user satisfaction but also build long-term brand credibility. From a policy and governance perspective, the research highlights a need for greater public engagement around data rights. While the Digital Personal Data Protection (DPDP) Act, 2023 represents a positive step, it remains poorly understood by most users. Policymakers must go beyond legislation to build public literacy campaigns, helping consumers understand their rights in simple, regional languages. A co-regulatory model, involving both the state and private firms, could enable more agile responses to emerging privacy challenges. Additionally, institutionalizing privacy-by-design across the tech and marketing industries, through certification systems, incentives, and training, could help shift the culture from reactive compliance to proactive ethics.

Despite these contributions, the study has several limitations. First, due to time and resource constraints, the interviews were limited to select urban and semi-urban regions. This may have excluded perspectives from rural users, whose experience of personalization and privacy may differ significantly. Second, language and class may have affected the depth of responses in some cases, as participants had varying levels of comfort discussing technical or abstract topics. Finally, the dynamic nature of AI technologies means that consumer attitudes and regulatory frameworks are likely to evolve, possibly limiting the study's long-term generalizability.

Future research could address these gaps by conducting comparative studies between youth and elderly users, or exploring platform-specific privacy practices on apps like Meta, Flipkart, or WhatsApp Business. Longitudinal studies that track how perceptions shift over time, particularly as laws like the DPDP Act gain traction, would also offer valuable insights.

In sum, this paper underscores that while AI personalization in India offers powerful tools for engagement, it must evolve alongside a cultural and legal infrastructure that respects privacy, encourages transparency, and empowers users to make informed choices.

CONCLUSION AND RECOMMENDATIONS

This study set out to explore how Indian consumers perceive AI-driven personalization in digital marketing and how they navigate the complex terrain of privacy in a rapidly digitizing society. The findings highlight a clear duality: on one hand, consumers enjoy the relevance, convenience, and efficiency that personalized content offers; on the other, they harbour concerns about how their data is collected, stored, and used, often without their full awareness or meaningful consent.

Rather than treating personalization and privacy as inherently conflicting goals, this study argues that they can, and must, coexist. Achieving this balance requires a shift in how personalization technologies are designed, communicated, and governed. Ethical design principles must prioritize transparency, control, and consent. Consumer education is equally vital, especially in a diverse society like India, where digital literacy varies significantly. Lastly, regulatory frameworks must not only exist on paper but function effectively in practice, with clear enforcement, accessible language, and public trust.

What emerges from this research is a call for more human-centered AI, systems that respect autonomy, reduce opacity, and recognize that consumers are not just data points, but individuals with rights, preferences, and lived experiences.

To align technological advancement with consumer protection, this study proposes the following recommendations:

Promote Privacy-by-Design Marketing Models

Marketers and developers should integrate privacy safeguards into the core of AI systems rather than as an afterthought. Features such as customizable personalization settings, real-time consent prompts, and clear data dashboards should become standard practice.

Standardize Privacy Notices and Opt-Out Mechanisms Privacy policies must be simplified, localized, and standardized across platforms to ensure accessibility and comprehension. Clear opt-out options, made visible at key decision points (not hidden in settings), will empower users to make informed choices.

Launch Nationwide AI and Privacy Literacy Campaigns

To close the gap between regulation and public understanding, targeted education campaigns should be rolled out, particularly in regional languages and through digital media, to raise awareness about data rights, consent, and AI-based profiling.

Strengthen Regulatory Bodies and Enforcement Mechanism

Institutions like India's Data Protection Board must be equipped with the resources, independence, and authority to enforce compliance and penalize

violations. A proactive, not reactive, regulatory stance is essential to keep pace with evolving technologies.

Together, these actions can build a more transparent, respectful, and inclusive digital ecosystem, one where personalization serves the user, not the other way around.

REFERENCES

1. Araujo, T., de Lima-Santos, M. F., & Vrancken, D. (2020). Does artificial intelligence have ethics? A study of consumer perceptions. *Journal of Business Ethics*, 167(4), 701–716. <https://doi.org/10.1007/s10551-019-04137-3>
2. Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342. <https://doi.org/10.1111/1540-4560.00067>
3. Dutta, P. (2023). An analysis of the Digital Personal Data Protection Act, 2023. *Indian Journal of Cyber Law & Policy*, 8(2), 56–68.
4. Farooq, M., Ramzan, M., & Yen, Y. Y. (2025). AI in consumer behavior management. In M. Farooq, M. Ramzan, & Y. Y. Yen (Eds.), *AI Applications in Marketing* (pp. 133–150). IGI Global.
5. Goyal, N., & Fernandes, A. (2024). India's data privacy journey: A comparative analysis with GDPR. *Data & Society Review*, 12(1), 33–49.
6. Hari, M. K., & Bibiyana, D. J. (2024). Consumer perception on the use of AI technology in digital marketing. *ResearchGate*. <https://www.researchgate.net/publication/387832655>
7. Kakodkar, P. (2023). Cultural dimensions of privacy in Indian digital users. *South Asian Digital Studies*, 5(1), 11–27.
8. Kietzmann, J., Paschen, J., & Treen, E. (2018). Artificial intelligence in advertising: How marketers can leverage AI. *Journal of Advertising Research*, 58(3), 263–267. <https://doi.org/10.2501/JAR-2018-035>
9. Kumar, A., & Sinha, R. (2022). AI-based personalization in e-commerce: A case study of Flipkart. *Indian Journal of Business Strategy*, 4(3), 41–55.
10. Mehta, R. (2023). What the DPDP Act 2023 means for Indian businesses and consumers. *The Economic and Political Weekly*, 58(27), 10–12.
11. Mitra, S., & Rathi, M. (2022). Consent fatigue and the illusion of control in digital India. *Journal of Media Studies*, 9(4), 103–118.
12. Nanda, S., & Pathak, H. (2021). AI-driven delivery platforms in India: Swiggy and the personalization paradox. *Asian Business Review*, 11(1), 24–35.
13. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
14. Raj, T., & Singh, V. (2023). Privacy dark patterns in Indian mobile apps: A qualitative audit. *Indian Journal of Information Technology Ethics*, 2(1), 44–59.
15. Saxena, R. (2023). The rise of AI in Indian fintech: Personalization and risk. *FinTech India Journal*, 7(2), 14–27.
16. Sayyed, A. A., Oberoi, S., & Kumari, A. (2025). Hyper-personalization of BFSI products in Pune: A narrative analysis. *JournalPress India*, 4(2), 66–75.
17. Sharma, D., & Iyer, P. (2024). Gamified AI personalization in Cred: A case study. *Journal of Marketing Innovation*, 6(1), 55–64.
18. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–560. <https://doi.org/10.2307/40041279>
19. Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
20. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.