# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

# DISCLAIMER

ISSN: 2582-6433

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# DATA-DRIVEN PRODUCT RECOMMENDATIONS AND CONSENT: A CORPORATE PERSPECTIVE ON AI, PRIVACY, AND COMPLIANCE UNDER INDIAN LAW

AUTHORED BY - MANYA B R & AJITHESH KUMAR
Christ University

## Abstract

In the era of Artificial Intelligence (AI), e-commerce platforms such as Amazon and Flipkart are increasingly using user responses for product recommendations. However, growing public concerns allege that these platforms might have access to sensitive personal information, such as audio conversations or text messages, without users' explicit consent. This paper critically examines from a corporate legal and ethical standpoint, particularly under the framework of India's Digital Personal Data Protection Act, 2023 (DPDPA). The purpose of the research is to assess whether the practices of data collection employed by these platforms align with the principles of valid, free, and informed consent and comply with lawful data processing standards by employing a doctrinal and analytical methodology. The findings suggest that, while public fears about unauthorised surveillance persist, there is no substantial legal or technological evidence to support such claims. The data used by these platforms is largely limited to user-consented behavioural inputs such as browsing patterns, purchase history, and search behaviour. Furthermore, most companies demonstrate compliance through practices like privacy by design, data minimisation, and offering user control mechanisms. The study concludes that despite these safeguards, the research identifies a significant trust gap rooted in insufficient transparency and user awareness.

**Keywords:** Artificial Intelligence, Corporate Compliance, Digital Personal Data Protection Act, E-commerce, Recommendation Systems,

## I. Introduction

The online shopping in India has gone through significant shifts, particularly due to the auto-recommendation systems that are used by most e-commerce platforms like Amazon and Flipkart. These systems process browsing history, past purchases, click behavior, and geographic information to customize the shopping experience. With each interaction, platforms

ISSN: 2582-6433

refine what products are shown and when, making the process more convenient and efficient. However, this personalization has raised privacy concerns. Many users worry that platforms may be accessing more information than they should, including private messages or call logs, mostly unverified claims, but highlight growing discomfort with how personal data is collected and used.

India's digital economy grows, so does the demand for stronger data protection. In response, the government introduced the Digital Personal Data Protection Act, 2023, which sets clear rules on how personal information is collected, stored, and used. A key focus of the law is informed user consent. Companies are now required to clearly explain what data they collect, why they collect it, and how it will be used, all in simple language. This moment calls for a serious evaluation of whether major e-commerce platforms are complying with these legal standards. The tension between personalization and privacy rights emphasizes the need for transparent and responsible data practices in a data-driven economy.

## II. Legal Framework: Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act[1], 2023 (DPDPA) is India's first comprehensive law aimed at regulating the collection, processing, storage, and transfer of personal data. The well-versed legislation is very important at a time when the country's digital economy is rapidly growing, particularly in sectors like e-commerce, where vast volumes of personal information are handled. The DPDPA Act puts individuals or data principals at the center of the data protection framework and outlines strict obligations for companies, known as data fiduciaries, regarding how personal information is managed.

A central pillar of the DPDPA is *consent*. As per Section 6[2], personal data must only be processed with clear and informed permission from the individual. According to the Act, consent must be voluntary, specific, and unambiguous, that is supported by a notice that explains what data is being collected, for what purpose, and how the individual can seek redress. The law prohibits silent consents, pre-checked boxes, or bundled approvals. Additionally, users have the right to withdraw consent at any time, after which the data must be deleted unless required for legal reasons. This provision is critical for platforms that rely on continuous user data collection.

[1] *Digital Personal Data Protection Act,2023, No.22, Acts Of Parliament,2023(India).*
[2] Digital Personal Data Protection Act,2023, § 6, No.22, Acts Of Parliament,2023(India).

ISSN: 2582-6433

The principles of *purpose limitation* and *data minimization*, outlined in Section 5[3], further restrict how companies handle data. Data fiduciaries or data holders are allowed to collect and process only the minimum amount of data necessary for a clearly stated purpose. For example, if a user's location is collected to display local sellers, that same data cannot later be used to infer income levels or habits without new and specific consent.

The Act also strengthens user rights. Section 11[4] states that the right to access their data and information about how it is used. Section 12[5] allows them to correct, update, or delete their information. Section 13[6] ensures grievance redressal within seven days. These measures ensure users have greater control and visibility over their data. However, the Act does not mandate full transparency on how data influences platform behavior; it does require companies to disclose what data is being used and why.

Sections 7[7] to 10[8] detail the responsibilities of data fiduciaries. Companies must ensure data accuracy, adopt strong security measures, and prevent unauthorized access. Section 8 introduces the concept of Significant Data Fiduciaries (SDFs), large-scale data handlers subject to stricter requirements, which also include the appointment of a Data Protection Officer (DPO), conducting regular audits, and performing Data Protection Impact Assessments (DPIAs). Majorly, the e-commerce platforms, given their operational scale and data practices, are likely to fall under this category.

To enforce the law, the Data Protection Board of India (DPBI) has been established. It has the authority to investigate breaches and impose penalties. The said Act further allowed the fines up to ₹250 crore for violations such as mishandling children's data or failing to prevent data breaches. This indicates a strong commitment to enforcement and emphasizes that non-compliance can result in serious financial consequences.

In comparison to the European Union's General Data Protection Regulation (GDPR), the DPDPA shares several principles, including informed consent, data minimization, and user

[3] Digital Personal Data Protection Act, 2023, § 5, No.22, Acts Of Parliament,2023(India).
[4] Digital Personal Data Protection Act, 2023, § 11, No.22, Acts Of Parliament,2023(India).
[5] Digital Personal Data Protection Act, 2023, § 12, No.22, Acts Of Parliament,2023(India).
[6] Digital Personal Data Protection Act, 2023, § 13, No.22, Acts Of Parliament,2023(India)
[7] Digital Personal Data Protection Act, 2023, § 7, No.22, Acts Of Parliament,2023(India)
[8] Digital Personal Data Protection Act, 2023, § 10, No.22, Acts Of Parliament,2023(India).

ISSN: 2582-6433

rights. However, unlike the GDPR, which allows multiple legal grounds for data processing. India's law focuses predominantly on consent, offering fewer exceptions[9]. This makes Indian companies more accountable but provides less operational flexibility. Additionally, the DPDPA leaves decisions regarding cross-border data transfers to government discretion under Section 16[10], which may create regulatory uncertainty for global businesses.

The PwC India Consumer Privacy Survey (2023) highlights widespread public concern, with 83% of respondents worried about their data being used without permission and 68% admitting to not reading privacy policies[11]. More than half of respondents falsely believe companies access private messages or listen to conversations. These findings underscore a serious gap in user understanding and the need for clearer communication by platforms.

To bridge this trust gap, companies must go beyond formal compliance. They should develop simplified, modular consent interfaces that allow users to manage different categories of data separately, such as location, browsing history, or purchasing patterns. These consent systems should be multilingual, easy to navigate, and offer examples of how data will be used.

Transparency reports are another step forward. Businesses should publish periodic summaries detailing what types of data were collected, how they were used, any third-party data sharing, and how many access or deletion requests were fulfilled. These reports could serve as industry benchmarks and help build public confidence.

Finally, the Data Protection Board of India should issue clear, sector-specific guidelines, particularly for industries[12] like e-commerce that handles large volumes of personal information. These guidelines should cover minimum standards for consent collection, data handling, and user rights enforcement. However, legal compliance alone is not enough. E-commerce platforms must earn consumer trust by prioritizing transparency, simplifying consent processes, and offering meaningful control over personal data. Only then can India achieve a fair balance between digital growth and individual privacy rights.

[9] Regulation (Eu) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 (General Data Protection Regulation), Art.6.
[10] Digital Personal And Data Protection Act,2023, §16, No.22, Acts Of Parliament, 2023(India).
[11] Pwc India, *Consumer Privacy Survey 2023*: India Insights 6 (2023).
[12] Digital Personal Data Protection Act, 2023, §19(2)(D),No.22, Acts Of Parliament,2023 (India).

ISSN: 2582-6433

## III. Technical Analysis of AI Recommendation Systems

AI-based recommendation systems have become a core feature of the e-commerce ecosystem. Platforms like Amazon, Flipkart, and Myntra rely on these systems to predict and suggest products that users are most likely to engage with or purchase[13]. Contrary to some public fears, modern recommendation systems do not rely on intrusive data like private conversations, phone messages, or call logs. Instead, they operate on defined models that process explicit and implicit user behavior within the boundaries of the app or website environment. This section explains the three primary models used in collaborative filtering, content-based filtering, and hybrid models, along with their standard data inputs, and uses this technical understanding to clarify misconceptions around data access and surveillance[14].

### 1. Collaborative Filtering

Collaborative filtering is one of the oldest and most widely used recommendation techniques. It functions on the principle that users who behaved similarly in the past will behave similarly in the future[15]. For example, if User A and User B both bought similar products in the past, and User A buys something new, the system may recommend that same product to User B.

There are two main types of collaborative filtering:

- **User-based filtering**, where the system finds similar users to the target user.
- **Item-based filtering**, where the system recommends items similar to those the user has interacted with.

These models depend heavily on explicit feedback (like product ratings) and implicit feedback (such as clicks, cart additions, purchase history, and time spent viewing items). No private data outside the platform is required. As noted by Ricci (2022), these algorithms depend on interaction matrices, typically sparse, which track user-item interactions on the platform itself. They are limited to data generated from within the e-commerce app, such as what the user browses, likes, or buys.

### 2. Content-Based Filtering

Content-based filtering takes a different approach by analyzing the attributes of the products themselves and matching them with a user's preferences. For instance, if a customer frequently

[13] Francesco Ricci, Lior Rokach & Bracha Shapira Eds., Recommender Systems Handbook (Springer 2022).
[14] Markus Zanker, Matthias Fuchs & Gunther Schoberegger, Recommender Systems In Tourism And Hospitality, 58 J.Travel Res. 544 (2019).
[15] Xiaoyuan Su & Taghi M. Khoshgoftaar, A Survey Of Collaborative Filtering Techniques, Advances In Artificial Intelligence 1 (2009).

ISSN: 2582-6433

buys cotton kurtas of a certain style or brand, the algorithm will recommend similar items that share those characteristics[16].

The key inputs for content-based models include:

- Product metadata (category, brand, material, color, price)
- User behavior (past purchases, product views, wishlists)
- Tags or keywords extracted from product descriptions

As emphasized by these systems use vector representations of items and user profiles, often calculated using techniques like TF-IDF or word embeddings, and then match user vectors with item vectors. Again, the model relies solely on platform activity and product data. No mechanism in such models accesses personal phone data, chats, or messages.

### 3. Hybrid Models

Hybrid recommendation systems combine collaborative and content-based methods to improve accuracy and reduce weaknesses inherent in using one model alone. They may use collaborative filtering for general popularity and personalization, and content-based filtering to fine-tune results to individual preferences. Some systems also include additional layers using contextual data, like location or time of day, to enhance the relevance of suggestions[17].

For example, Amazon's hybrid system may recommend a mobile phone based on your browsing history (collaborative filtering), and then refine suggestions based on the product specifications you typically prefer (content-based).

Hybrid systems often use machine learning classifiers or matrix factorization techniques, such as singular value decomposition (SVD), to build a comprehensive user profile. In more advanced cases, deep learning models like neural collaborative filtering (NCF) or transformers are used, which still rely on the same basic data inputs: what the user did on the platform, not what the user says elsewhere.

### 4. Common Data Inputs Used in Recommendation Systems

All major recommendation systems, regardless of the model, rely on structured, platform-generated data. Typical data inputs include[18]:

- Browsing history (pages visited, session durations)

[16] Pasquale Lops, Marco De Gemmis & Giovanni Semeraro, Content- Based Recommender Systems: State Of The Art And Trends, In Recommender Systems Handbook (Francesco Ricci Et Al. Eds., Springer 2011).
[17] Robin Burke, Hybrid Recommender Systems: Survey And Experiments, 12 User Modeling & User-Adapted Interaction 331 (2002).
[18] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India).

ISSN: 2582-6433

- Search queries (keywords used on the platform)
- Clickstream data (clicks on product listings, categories)
- Purchase history (items bought, returned, or reviewed)
- Wishlist or saved items

Data pipelines ingest these behavioral signals and convert them into features for the recommendation model. As clarified in AWS's Machine Learning documentation, all data is collected through user interactions within the app or website, and usage is tied to what the platform logs, not third-party or private data sources.

**5. Addressing Public Concerns: No Evidence of Accessing Private Communications**

A common public concern in India, often discussed on social media and anecdotal forums, is the idea that e-commerce apps "listen" to private conversations or read messages to recommend products. For instance, someone may discuss "buying a coffee maker" with a friend and later receive an ad for one, prompting fears of surveillance[19].

From a technical standpoint, these claims are not supported by the architecture of real-world recommender systems. E-commerce platforms do not have access to private messaging apps (like WhatsApp or SMS) unless explicitly granted by the user, something Android and iOS security models do not permit by default. Moreover, privacy rules enforced by app marketplaces have significantly limited access to call logs and message data, especially post-Android 10 and iOS 14.

Also, natural correlation plays a large role. Many platforms track a wide range of user behavior, including search patterns, purchase intent signals, and social browsing behavior. If a user searched for a coffee mug on Google, saw similar items on Instagram, and then opened Flipkart, product suggestions could be based on cookies or inferred intent across platforms, but not necessarily private conversations[20].

Additionally, most recommendation engines work offline or on the server-side, processing pre-existing data rather than live surveillance. None of the models (collaborative, content-based, or hybrid) includes architecture to receive or process audio or private text inputs unless explicitly enabled by the user, for example, in smart assistant devices like Alexa or Google Assistant, which operate under different consent structures.

AI-powered recommendation systems function on well-established algorithms that use behavioral data generated within the boundaries of a given platform. These systems do not rely

[19] Pwc India, Consumer Privacy Survey 2023: India Insights (2023).
[20] Google, Android 10 Privacy Changes, Google Developers Blog (2020).

ISSN: 2582-6433

on private messages, phone conversations, or unauthorized access to personal data. Models like collaborative filtering, content-based filtering, and hybrid approaches use structured inputs such as browsing activity, purchase records, and product metadata, none of which require intrusion into private communications[21].

Understanding the technical framework of these systems helps clarify that the fears of constant surveillance are largely rooted in correlation rather than causation. Transparency and better communication from companies about how their recommendation engines work will be crucial in rebuilding user trust under India's evolving data protection laws.

## IV. Corporate Compliance with DPDPA

With the enforcement of the DPDPA, Indian e-commerce platforms face clear legal obligations regarding how they collect, process, and manage personal data[22]. Sections such as Section 6 (consent), Section 5 (purpose limitation and data minimization), and Sections 11 to 13 (user rights) impose duties that directly affect AI-driven product recommendation systems. This section analyzes how two major platforms, Amazon India and Flipkart, align with the DPDPA based on their publicly available privacy policies, focusing on consent mechanisms, privacy by design, and specific user controls such as deletion and opt-out options.

### 1. Amazon India: Consent and User Controls

Amazon India's Privacy Notice outlines its data collection practices covering browsing activity, device info, search queries, and order history, but falls short of what the Digital Personal Data Protection Act, 2023 (DPDPA) demands[23]. The company's approach to consent is broad and implicit, relying on a general statement:

*"By using our Services, you agree to our use of your personal information[24]..."*

This bundled consent doesn't meet Section 6[25] of the DPDPA, which requires that consent be clear, specific, and informed. There's no option for users to choose how different categories of their data, like location or behavioral insights, are used, which undermines the purpose-specific consent model required by the law[26].

[21] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India).
[22] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India).
[23] F. Ricci, L. Rokach & B. Shapira, Recommender Systems Handbook 18–25 (2d Ed., Springer 2022).
[24] Amazon India, Amazon India Privacy Notice, Https://Www.Amazon.In/Gp/Help/Customer/Display.Html?Nodeid=Gx7njq4zb8mhfrnj (Last Visited Mar. 10, 2026).
[25] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India) § 6.
[26] Rolf H. Weber & Romana Weber, Internet Of Things: Legal Perspectives 73–78 (Springer 2010)

ISSN: 2582-6433

Amazon does provide some user rights tools. Its "Request Data Deletion[27]" feature aligns with the right to erasure under Section 12, but lacks clarity on what data is retained and why. Similarly, the "Download Your Data" option supports Section 11's right to access, though users have reported delays, something that could conflict with Section 13's grievance redressal timeline.

Overall, Amazon's privacy controls prioritize convenience over compliance. The settings are hard to find, and the consent is assumed rather than actively given. For everyday users, this setup makes it difficult to understand, control, or limit how their data is used, putting Amazon at odds with both the letter and spirit of the DPDPA.

**2. Flipkart: Opt-Out and Granular Controls**

Flipkart's Privacy Policy is more explicit in detailing the categories of data collected and includes a separate section on user choices and rights. It lists data such as IP address, device ID, transaction history, and location data. Flipkart mentions:

"*You may choose to opt out of promotional communications, and can manage your preferences under account settings.*"[28]

This opt-out model, however, falls short of the opt-in consent standard under Section 6[29] of the DPDPA. Consent under the Act must be collected before data processing, not presumed and later revoked. Flipkart does not offer consent segmentation for specific purposes such as AI personalization or behavioral tracking. All user data is processed based on general platform use, which can be challenged under the DPDPA's purpose limitation rule in Section 5(1).

Flipkart does enable users to disable location access, and the app requests permission explicitly when first opened, a positive step toward compliance. However, this is enforced at the device level, relying on OS-level settings rather than offering Flipkart's data-specific consent mechanism.

Importantly, Flipkart does not currently provide a clear, direct "Delete My Data" option, as Amazon does. Requests for account deletion can be initiated via customer support, but the privacy policy lacks a self-service tool. This could result in non-compliance with Section 12, which guarantees users the ability to request deletion of data that is no longer necessary for the purpose for which it was collected.

On access rights, Flipkart allows users to view and correct basic profile information such as

[27] Daniel J. Solove, Understanding Privacy 105 (Harvard Univ. Press 2008).
[28] Flipkart, Privacy Policy, Https://Www.Flipkart.Com/Pages/Privacypolicy (Last Visited Mar. 10, 2026).
[29] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India) § 6.

ISSN: 2582-6433

name and address. However, more detailed behavioral data, such as search history, recommendation logs, or cross-session profiling data, are not made accessible. Under Section 11, such profiling data, especially if used to influence user decisions, must be disclosed upon request.

### 3. Privacy by Design: Structural Observations

Neither Amazon nor Flipkart explicitly mentions privacy by design or by default, a concept embedded in global data protection standards and expected implicitly under the DPDPA's Section 7[30], which mandates reasonable safeguards and accountability. Platforms should ideally implement systems where privacy settings are enabled by default and where users are nudged toward informed decisions, not buried in complex menu trees. The current practice of hiding data preferences under multiple tabs or within lengthy privacy policies is more aligned with compliance formalism than with actual user empowerment.

From an ethical standpoint, this gap between legal text and user experience reinforces the argument that consumer trust depends not only on compliance but on perceived control and fairness[31]. Users tend to feel manipulated when consent is a prerequisite for access, but not a genuine choice, something both Amazon and Flipkart risk if they continue with generalized, non-specific data consent mechanisms.

### 4. Ethical and Legal Risk Assessment

Amazon India and Flipkart have endeavored to adapt to changing privacy standards, yet their actions still do not achieve complete adherence to the DPDPA[32]. A major concern is their dependence on general, implied consent automatically presumed when users start using the platforms rather than providing detailed, opt-in options for particular purposes such as behavioral tracking, profiling, or targeted promotions[33]. This directly violates Section 6, which requires explicit, detailed, and informed consent[34]. Moreover, both organizations seem to contravene the principle of purpose limitation under Section 5 by not adequately distinguishing between the different purposes of data processing. Their general disclosures fail to adequately guarantee that data is utilized solely for lawful, specified purposes or restricted to what is

[30] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India) § 7.
[31] Patricia A. Norberg Et Al., The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors, 41 J. Consumer Aff. 100 (2007). 41 *Journal Of Consumer Affairs* 100–126 (2007).
[32] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India) § 6.
[33] Amazon India, Amazon India Privacy Notice, Https://Www.Amazon.In/Gp/Help/Customer/Display.Html?Nodeid=201909010 (Last Visited July 25, 2025).
[34] Pwc India, Consumer Privacy Survey 2023: India Insights 4 (2023).

ISSN: 2582-6433

essential[35]. Moreover, both platforms lack provision for users to obtain more detailed insights like behavioral profiling or recommendation history, undermining their adherence to Section 11's right to access.

Regarding user rights and grievance redressal, Amazon outperforms Flipkart by providing features such as "Request Data Deletion" and "Download Your Data," which aid in adhering to Sections 11 and 12. In comparison, Flipkart does not offer clear, self-service methods for users to delete their personal information, complicating the process for individuals to assert their rights. Mechanisms for addressing grievances under Section 13 are insufficiently handled by both platforms. Amazon fails to define resolution timelines, and Flipkart relies on broad customer support protocols. Furthermore, neither organization has significantly embraced a privacy-by-design methodology, as anticipated in Section 7. Privacy settings frequently hide within intricate menus, and default options usually prioritize data collection rather than safeguarding[36]. Although Amazon provides a bit more control, both firms regard compliance as a mere checkbox task instead of a commitment focused on the user. Without a transition to clear, reversible consent frameworks and active privacy protections, they face potential legal consequences and a decline in consumer confidence in India's growing privacy-aware digital environment[37].

## V. Addressing the Trust Gap and Transparency

As digital shopping platforms like Amazon and Flipkart continue to personalize user experiences using data-driven technologies, many Indian consumers are becoming increasingly uneasy about how their data is being collected and used. While the convenience of AI-based recommendations is marketed as a benefit, people often feel unsure about what's happening behind the scenes. This lack of clarity is made worse by complicated privacy policies and countless personal stories shared online, especially on platforms like X (formerly Twitter), where users say they feel like these platforms are "listening" to their conversations or "reading" messages[38]. Even if these fears aren't always technically accurate, they show how deeply people feel the loss of control over their digital lives[39]. The Digital Personal Data Protection Act, 2023 (DPDPA), was introduced to tackle exactly this kind of public concern.

[35] Amazon, Download Your Data, Https://Www.Amazon.In/Gp/Help/Customer/Display.Html?Nodeid=202075050 (Last Visited Mar. 10, 2026).
[36] Shoshana Zuboff, The Age Of Surveillance Capitalism (Publicaffairs 2019).
[37] Omer Tene & Jules Polonetsky, Big Data For All: Privacy And User Control In The Age Of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013).
[38] Alessandro Acquisti Et Al., Privacy And Human Behavior In The Age Of Information, 347 Science 509 (2015).
[39] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India) Pmbl.

ISSN: 2582-6433

A quick look at conversations on X reveals how widespread this anxiety has become. Posts under hashtags like "Amazon privacy India" or "Flipkart data concerns" often describe eerily timed ads. People mention a product in a chat or SMS, and suddenly they see it promoted online. While this may be the result of predictive algorithms or ad tracking rather than spying, users still feel watched[40]. One popular post from October 2023 summed it up: "Had a private chat with a friend about running shoes. Didn't search anywhere. The next day, Amazon pushes running shoes in my feed. Are they reading my messages?" Even if there's a technical explanation, the emotional takeaway is clear: people are uncomfortable, and that matters[41].

This discomfort isn't just anecdotal. According to the 2023 PwC India Consumer Privacy Survey, a massive 83% of users worry that their data is being used without their consent, and 68% admit they don't even read privacy policies[42]. Shockingly, over half of the respondents wrongly believe that companies are reading their private messages or listening in on conversations. These misunderstandings show that people's concerns aren't only about what's happening, they're also about what companies *aren't* saying[43]. The lack of clear communication, paired with low digital literacy around how data and AI work, is fueling public distrust[44].

Experts have pointed to this issue for years. Alessandro Acquisti's widely cited research calls it the "privacy paradox": people say they care about their privacy, but often act against their interests[45]. This isn't hypocrisy, he argues, it's confusion. When platforms overwhelm users with technical language or bury important information, users default to distrust[46]. In India, the problem is even worse. With dozens of languages, a mobile-first population, and historically weak privacy enforcement, users are often left to navigate a complex digital world with little guidance. The result? A widening trust gap between users and platforms.

To close that gap, companies need to go beyond just checking legal boxes. Transparency needs to become part of the user experience. That means creating simple, multilingual tools where

[40] Patricia A. Norberg Et Al., The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors, 41 J. Consumer Aff. 100 (2007).
[41] Omer Tene & Jules Polonetsky, Big Data For All: Privacy And User Control In The Age Of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013).
[42] Pwc India, Consumer Privacy Survey 2023: India Insights 6–7 (2023).
[43] Daniel J. Solove, Understanding Privacy 105 (Harvard Univ. Press 2008).
[44] Rolf H. Weber & Romana Weber, Internet Of Things: Legal Perspectives 73–78 (Springer 2010).
[45] Supra Note 31
[46] Solove, Supra Note 36.

ISSN: 2582-6433

people can choose what kinds of data they want to share, like browsing history, location, or purchase habits, with clear examples of what changes if they opt out. It also means publishing plain-language reports that show how data is used and shared, and how many user requests for data deletion or access were honored. Just as financial firms report on sustainability, tech platforms should report on data use. Finally, government regulators should step in with strong guidelines and surprise audits to keep companies honest[47]. At the end of the day, winning back trust will require more than promises; it demands openness, empathy, and a genuine respect for users' rights[48].

## VI. Ethical AI and Innovation vs. Accountability

As artificial intelligence becomes central to the evolution of e-commerce in India, platforms like Amazon and Flipkart are increasingly relying on machine learning to personalize user experiences, from recommending products to shaping the entire shopping journey. While this enhances engagement and drives sales, it also raises pressing ethical questions about privacy, fairness, and accountability[49]. AI-driven systems frequently operate in ways that are opaque and unchecked, pushing the boundaries of legal frameworks like the DPDPA[50]. These systems gather, analyze, and act on vast amounts of user data without always offering clear consent choices or transparency, creating a conflict between technological efficiency and individual rights[51].

A major concern in this landscape is the erosion of fairness. AI algorithms often treat users as patterns to be predicted rather than individuals with autonomy and dignity. Though this data-driven approach may improve business performance, it clashes with DPDPA principles like informed consent, purpose limitation, and data minimization[52]. Personal data should only be used for specific, lawful purposes, but adaptive AI models blur those lines, evolving with user behavior while bypassing renewed consent or clearly stated intentions[53]. Moreover, AI's black-box nature means companies themselves may not fully understand or explain the decisions their systems make, further challenging the requirement under Section 7 of the DPDPA for privacy-

[47] Upendra Baxi, The Rule Of Law In India: Theory And Practice, 23 J. Indian L. Inst. 1 (1981).
[48] Shoshana Zuboff, The Age Of Surveillance Capitalism (Publicaffairs 2019).
[49] Robin Burke, Hybrid Recommender Systems: Survey And Experiments, 12 User Modeling & User-Adapted Interaction 331 (2002).
[50] Digital Personal Data Protection Act, 2023, No. 22, Acts Of Parliament, 2023 (India) §§ 5–7.
[51] Xiaoyuan Su & Taghi M. Khoshgoftaar, A Survey Of Collaborative Filtering Techniques, Advances In Artificial Intelligence 1 (2009).
[52] F. Ricci, L. Rokach & B. Shapira, Recommender Systems Handbook 18–25 (2d Ed., Springer 2022).
[53] Markus Zanker Et Al., Recommender Systems In Tourism And Hospitality, 58 J. Travel Res. 544 (2019).

ISSN: 2582-6433

by-design and responsible data governance[54].

To correct this imbalance, companies must integrate ethical safeguards into the very foundation of AI development. Institutionalising ethical AI audits and algorithmic impact assessments is a key step forward[55]. These mechanisms should evaluate how recommendation engines use data, whether consent standards are maintained, and whether outcomes may inadvertently reinforce discrimination or exclusion[56]. Internal teams or independent bodies can conduct these audits, followed by transparent reporting of the results and corrective actions. Algorithmic impact assessments, conducted during design stages, can help predict and mitigate risks such as over-profiling or biased targeting, especially in sensitive areas like health, finance, or gender-based products, ensuring AI remains accountable to user well-being and legal standards[57].

Regulatory intervention must accompany corporate efforts. The Data Protection Board of India should develop sector-specific rules for AI transparency and enforce regular compliance reviews, especially for systems that significantly affect user autonomy or service access[58]. Enforcement should be swift, proportionate, and publicly visible to hold companies accountable and deter negligent practices[59]. Companies must recognise that ethical compliance isn't a burden but a strategic advantage[60]. Platforms that embed transparency, accountability, and user empowerment into their AI systems are more likely to earn long-term consumer trust, enabling responsible innovation that is proactive rather than reactive in addressing India's emerging data protection landscape[61].

[54] Pasquale Lops Et Al., Content-Based Recommender Systems: State Of The Art And Trends, In Recommender Systems Handbook 73 (F. Ricci Et Al. Eds., Springer 2011).
[55] Brent Mittelstadt Et Al., The Ethics Of Algorithms: Mapping The Debate, 3 Big Data & Soc'y 1 (2016).
[56] Andrew D. Selbst & Solon Barocas, The Intuitive Appeal Of Explainable Machines, 87 Fordham L. Rev. 1085 (2018).
[57] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why A Right To Explanation Of Automated Decision-Making Does Not Exist In The General Data Protection Regulation, 7 Int'l Data Privacy L. 76 (2017).
[58] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act), Com (2021) 206 Final (Apr. 21, 2021).
[59] Reuben Binns, On The Apparent Conflict Between Individual And Group Fairness, In Proceedings Of The 2020 Conf. On Fairness, Accountability, & Transparency 514 (2020).
[60] Shoshana Zuboff, The Age Of Surveillance Capitalism (Publicaffairs 2019).
[61] Tene O. & Polonetsky J., Big Data For All: Privacy And User Control In The Age Of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 245 (2013).

ISSN: 2582-6433

## VII. Conclusion & Recommendation

The analysis of product recommendation systems in India's e-commerce sector, particularly those used by Amazon and Flipkart, reveals a pressing gap between regulatory compliance and public trust. Although both companies have introduced measures in line with the Digital Personal Data Protection Act, 2023 (DPDPA), such as publishing privacy policies, offering consent options, and providing tools for data deletion, these steps have not translated into user confidence. The prevailing concern among users stems from opaque consent mechanisms, limited control over personal data, and a widespread lack of understanding about how their information is used for personalisation. Consent remains bundled and vague, often buried in lengthy terms and conditions that are neither accessible nor informative, especially for users with limited digital literacy. This disconnect is further exacerbated by anecdotal experiences shared on social media, where users interpret personalised suggestions as surveillance, reinforcing feelings of being profiled without explicit permission.

To bridge this trust gap, platforms must move beyond formal compliance and prioritise ethical data practices and transparency. This includes developing clear, modular consent interfaces that allow users to selectively opt in or out of specific data uses, as well as publishing regular transparency reports detailing what data is collected, why, and with whom it is shared. Routine audits of recommendation algorithms, both internal and independent, should ensure adherence to consent, avoid discriminatory outcomes, and reinforce purpose limitation. These technical reforms must be supported by government-led public awareness campaigns, especially by MeitY, using simple language and culturally relevant content to educate users about their rights under the DPDPA. Additionally, sector-specific standards and random audits by the Data Protection Board will be essential for sustained enforcement. Ultimately, while legal frameworks like the DPDPA lay the foundation, long-term accountability and responsible digital commerce in India will depend on transparent corporate practices and collaborative regulatory oversight.