Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Digital Brand Enforcement Under the DPDPA: Balancing Intellectual Property Protection and Data Privacy in India

Palak Chauhan[a]

[a]Law Graduate, Faculty of Law, University of Delhi, Delhi, India

Received 29 May 2026; *Accepted* 30 June 2026; *Published* 04 July 2026

In India, reliance on data is increasing for digital brands. To detect counterfeits, trademark violations, impersonation, and deceptive business practices, brand owners, law firms, and investigators are now monitoring e-commerce listings, social media profiles, domain names, paid advertisements and online marketplaces to detect counterfeit goods, trademark infringement, impersonation and misleading commercial activity. These enforcement methods often require collecting and utilising personal information such as seller names, phone numbers, account IDs, addresses, screenshots, invoices, transaction records, and communications from the platform. Therefore, the Digital Personal Data Protection Act, 2023 affects India's digital brand enforcement techniques. This article argues that the DPDPA does not prevent brand enforcement. It rather requires that enforcement be more balanced and privacy-compliant. The Act recognises legal data processing exceptions for maintaining legal rights and for investigating violations or legal transgressions. It also imposes duties to purpose limitation, security measures, processor management and accountability. The article discusses the relationship between data protection, trademark enforcement, intermediary liability, and privacy-by-design, and advises using the latter to protect digital brands. It concludes that data privacy and intellectual property protection are both essential to building consumer confidence in the digital market and are not mutually exclusive.

Keywords: *data protection, digital brand enforcement, trademarks, counterfeiting, intermediary liability.*

INTRODUCTION

Digital markets have transformed the brand's production, marketing, and misuse. Brand infringement extends beyond store signs, imitation merchandise or printed advertisements. It currently manifests on social media profiles, ads, e-commerce listings, fake websites, impersonation accounts, messaging apps and domain names. Counterfeit vendors might change product photos, use many IDs, move between markets, and keep selling even after an account is closed. Hence, brand owners have to constantly work to enforce online.

Given the present changes, brand enforcement nowadays depends much on data. A trademark owner could compile information like seller usernames, product URLs, phone numbers posted on social media, delivery labels, invoices, payment references, customer complaints, and platform communications—screenshots of violating listings. Using this information, law companies can file criminal charges, seek injunctions, demand seller information disclosure, file lawsuits, or issue takedown notices. Investigation agencies may conduct trap purchases or gather reports on sellers. These steps are essential for modern brand protection, but they also involve processing personal data.

The Digital Personal Data Protection Act 2023 ('DPDP Act') oversees digital personal data handled inside India and, in particular circumstances, also covers processing done outside India when it pertains to offering goods or services to Data Principals in India.[1] The Act defines personal data as any information about an individual who can be directly or indirectly identified from that data. Processing includes operations such as collection, recording, storage, use, sharing, and erasure. As a result, many routine brand-enforcement practices may fall within the scope of data protection law.

This article argues that the DPDP Act does not impede digital brand enforcement. It offers internet infringers or counterfeiters no protection from legitimate legal action. However, it changes how enforcement must be conducted. Enforcement must be lawful, necessary, documented, secure and proportionate. The main concern is not whether brand owners may process data for enforcement, but how they can do so without violating data protection guidelines.

[1] Digital Personal Data Protection Act 2023

DIGITAL BRAND ENFORCEMENT USING PERSONAL DATA

Digital brand enforcement refers to the identification, documentation and removal of online misuse of a brand. It may involve actions for trademark infringement, passing off, counterfeiting, domain name misuse, phishing, impersonation, misleading advertisements and copyright infringement. Intellectual property laws guide such behaviour. The Trade Marks Act of 1999 gives a registered proprietor exclusive rights and legal remedies in case of infringement.[2] Original works are protected by the Copyright Act 1957; it also grants remedies for unauthorised use.[3]

In practice, these rights cannot be enforced without evidence. Online infringement is frequently short-lived and readily removed. Therefore, a brand owner must document the infringing listing, the seller's identity, the date of access, product images, pricing, product description, reviews, and any publicly visible contact information for customers. In cases involving counterfeits, a trap purchase may be necessary to prove that the advertised product is not authentic. Such a purchase may result in invoices, delivery records, photos of packaging, courier information and seller addresses.

Some of this information may pertain to businesses. Nonetheless, most online sellers are sole proprietors, small traders, individual resellers and account holders. The seller's name, phone number, email address, photo, address and payment code may identify them. A username may be treated as personal data if it can be linked to a particular individual. Therefore, digital brand enforcement cannot presume that seller information is entirely commercial. It frequently lies at the crossroads of commercial investigation and personal data processing.

Personal data generated or caused to be generated and made publicly available by the Data Principal herself or by someone lawfully required to reveal it publicly is significantly excluded from the DPDP Act.[4] This is relevant when a seller voluntarily adds contact details on a social media page or in a public market listing. The public-data exclusion does not, however, provide unlimited permission to collect everything available online. The exclusion may not apply to information gathered from platform backends, private messages, KYC requests, test purchases, or databases supplied by third-party investigation firms. Therefore,

[2] Trade Marks Act 1999
[3] Copyright Act 1957
[4] Digital Personal Data Protection Act 2023

a stringent enforcement plan should assume that personal data is regulated unless a clear exception is expressly applied.

LAWFUL PROCESSING AND THE LIMITS OF CONSENT

It is commonly misunderstood that data protection law requires consent for every type of data processing. The DPDP Act allows personal data to be processed for a lawful purpose, either with the individual's consent or for specific legitimate reasons. In brand enforcement, obtaining consent from the suspected infringer is typically neither feasible nor preferred. Requesting permission from suspected counterfeiters to gather evidence would undermine the investigation.

The more pertinent question is whether the processing serves a lawful purpose. A lawful purpose must not be forbidden by law. Examples of lawful purposes include protection of trademarks, investigation of counterfeit goods, removal requests, injunctions and preventing consumer fraud. However, merely having a lawful purpose should not excuse unlimited collection. The DPDP Act also adopts a necessity-based approach, especially in the framework of consent and various obligations placed on Data Fiduciaries. Even when consent is not the primary basis, the discipline of necessity still proves valuable.

For instance, when a brand owner is recording an infringing e-commerce listing, it may need to gather the product image, the infringing mark, the seller's name, the URL, the listing date, and the transaction details. It may not be necessary to gather unrelated buyer comments, personal user photos, or unrelated products sold under the same account. To demonstrate misuse of a trademark, the evidence must be confined to that specific purpose. This is not only privacy-compliant but also improves the quality of legal evidence.

Thus, the DPDP Act promotes a move from broad surveillance to targeted enforcement. Each investigation, whether takedown, litigation, criminal complaint, customs action, consumer warning, or internal risk assessment, should have a clearly defined purpose from the brand owner. The types of personal data collected should then be linked to that purpose. This demonstrates that enforcement was neither arbitrary nor excessive.

EXEMPTIONS FOR LEGAL RIGHTS AND INVESTIGATION OF CONTRAVENTIONS

The key provisions for brand enforcement are the exemptions outlined in Section 17 of the DPDP Act. Section 17 provides an exemption for specific processing when it is necessary to enforce a legal right or claim.[5] It also exempts processing carried out for the purpose of preventing, detecting, investigating, or prosecuting any offence or contravention of law.

These provisions are significant because digital brand enforcement is, by its nature, connected with legal rights. Civil lawsuit, statutory penalty, and, on rare occasions, criminal charge can arise from the likes of trademark infringement, passing off, copyright infringement, sale of counterfeit goods, and false business advertising. So, a brand owner assembling evidence to file a suit, issue a cease-and-desist notice, a takedown request, or an investigative request is backed by an unequivocal legal right to the benefit or reliance on the provisions.

Nevertheless, the term "necessary" holds significance. The exemption does not grant general authorisation for indiscriminate monitoring. It safeguards processing that is truly linked to legal enforcement. If a brand owner collects a suspected infringer's name, phone number, and address for potential legal action, that may be reasonable. If it compiles a database of unrelated consumers who commented on a suspicious post, that could be considered excessive. The exemption should therefore be applied using a purpose-and -necessity test.

This interpretation is also in consonance with the constitutional right to privacy as recognised in Justice KS Puttaswamy v Union of India.[6] Privacy is not absolute, but any intrusion into it must be lawful, have a legitimate purpose and be proportionate. Brand enforcement is meant to protect the goodwill, preclude consumer confusion and prevent the manufacturing and distribution of counterfeit products. But private enforcement must not become private surveillance. The DPDP Act can be seen as a statutory framework that disciplines enforcement without undermining it.

[5] Digital Personal Data Protection Act 2023, s 17

[6] *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

PLATFORM TAKEDOWNS, SELLER DISCLOSURE AND INTERMEDIARY LIABILITY

Digital brand enforcement often depends on intermediaries. E-commerce marketplaces, social media platforms, domain registrars and payment intermediaries have information that brand owners may need to identify infringers. Intermediaries enjoy a conditional safe harbour under the Information Technology Act 2000 as long as they meet statutory requirements.[7] It also requires intermediaries to observe due diligence under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.[8]

Indian courts have considered the responsibilities of intermediaries in cases involving online infringement. In Shreya Singhal v Union of India, the Supreme Court read down the concept of "actual knowledge" under Section 79 of the IT Act in a manner that required such knowledge to be established through a court order or official notification issued by the appropriate government or agency, as understood by the Court in that context.[9] In MySpace Inc v Super Cassettes Industries Ltd, the Delhi High Court examined copyright enforcement against an online platform and acknowledged the necessity of balancing copyright protection with the intermediary safe harbour.[10] In Kent RO Systems Ltd v Amit Kotak, the Delhi High Court refused to impose a general obligation on an intermediary to proactively screen all products for intellectual property infringement.[11] In Christian Louboutin SAS v Nakul Bajaj, the Delhi High Court examined when an e-commerce platform may move beyond passive intermediary status and become actively involved in the transaction.[12]

The DPDP Act introduces a privacy dimension to these issues. Takedown requests may indeed require a party to be able to store data about the seller, the complainant and the user. Requests for revealing the seller's identity may require personal data like name, address, telephone number, KYC and transaction data. In the absence of law, contractual provisions, court orders, government requests or a clear basis to exercise legal rights, parties may be reluctant to provide such data.

---

[7] Information Technology Act 2000
[8] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[9] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[10] *My Space Inc v Super Cassettes Industries Ltd* (2017) 236 DLT 478
[11] *Kent Ro Systems Ltd & Anr v Amit Kotak & Ors* (2017) SCC OnLine Del 7201
[12] *Christian Louboutin SAS v Nakul Bajaj & Ors* AIRONLINE (2018) Del 1962

This does not imply that brand owners are unable to request disclosure. It implies that disclosure requests must be drafted with precision. A strong takedown notice should identify the trademark registration number, the infringing URLs, screenshots, nature of infringement, likelihood of consumer confusion, and a request for the specific remedies sought. If seller information is requested, the notice must clarify why it is needed to enforce legal rights or investigate a legal contravention. Vague requests for "all seller data" are more likely to trigger privacy concerns. Requests aimed at obtaining specific identifiers needed for legal action are more justifiable.

EVIDENCE PRESERVATION, RETENTION AND SECURITY

Digital evidence is fragile. Listings disappear, advertisements expire, usernames are changed, and sellers take down infringing content after being notified. Therefore, brand owners must promptly preserve evidence. Concurrently, the DPDP Act requires Data Fiduciaries to ensure personal data is safe, implement technical and organisational measures in place, and erase personal data when the specified purpose is no longer served unless retention is necessary for compliance with law.

This creates a practical tension. Deleting enforcement data too early could cause a brand owner to lose crucial evidence needed for litigation. Storing data indefinitely may breach data protection principles. The solution is a structured retention policy. Evidence for ongoing disputes, repeat offenders, police reports and pending civil suits can be stored as long as necessary. Personal data that is irrelevant to the purpose of monitoring must be deleted or anonymised once the purpose is served.

The DPDP Rules 2025 also make security central to compliance. Rule 6 requires reasonable security measures, such as encryption, obfuscation or masking, access controls, logging, monitoring, backup, processor contracts and technical and organisational safeguards.[13] Rule 7 deals with intimation of personal data breach to affected Data Principals and the Data Protection Board.[14] Rule 8 addresses erasure and retention under certain specified conditions.[15]

[13] Digital Personal Data Protection Rules 2025, r 6
[14] Digital Personal Data Protection Rules 2025, r 7
[15] Digital Personal Data Protection Rules 2025, r 8

These rules have immediate effects on brand protection databases. A spreadsheet listing suspected seller identities, phone numbers, addresses, invoices, and payment references should not be circulated casually. Access must be restricted to legal and enforcement teams. Investigation reports must be stored securely. Access for vendors should be managed carefully. Evidence should be preserved with records of date, time, source, and chain-of - custody. These measures not only reduce privacy risks but also strengthen the credibility of evidence in court.

VENDORS, CROSS-BORDER DATA SHARING AND CHILDREN'S DATA

Many brand owners outsource enforcement to law firms, investigators, monitoring vendors, software providers and overseas brand-protection teams. Under the DPDP Act, a Data Fiduciary is still accountable for any data processing carried out on its behalf by a Data Processor. It may engage a Data Processor only through a valid contract for processing connected with offering goods or services to Data Principals. Thus, effective vendor management is crucial.

Contracts with brand-protection vendors should specify the purpose of data processing, types of data involved, confidentiality obligations, security measures, breach reporting, data retention period, obligations for data deletion, and restrictions on onward sharing. Investigators should be directed to collect only the essential information. For example, during a trap purchase, collecting the seller's invoice and return address may be justified, but collecting unrelated personal conversations or customer data may not be.

Cross-border sharing also requires attention. Numerous companies employ global enforcement dashboards, uploading Indian data for review by regional or international teams. The DPDP Act allows the Central Government to impose restrictions on the transfer of personal data to specified countries or territories. Rule 15 of the DPDP Rules 2025 further states that transfers outside India are subject to requirements that the Central Government may specify in relation to making personal data available to foreign States or entities controlled by them.[16] Therefore, brand owners should document cross-border workflows and minimise identifiable data shared with foreign affiliates unless necessary.

[16] Digital Personal Data Protection Rules 2025, r 15

Children's data is another sensitive domain. Certain infringing activities involve toys, gaming products, educational apps, children's entertainment, or social media pages followed by minors. The DPDP Act limits the processing of children's personal data and prohibits tracking, behavioural monitoring, and targeted advertising directed at children.[17] Brand enforcement in such matters should target infringing content, the identity of sellers, and the actions taken by platforms not profiling child users or gathering unnecessary data from minors.

TOWARDS A PRIVACY-BY-DESIGN BRAND ENFORCEMENT MODEL

The DPDP Act should be seen as an opportunity to professionalise digital brand enforcement. A privacy-by-design approach enables brand owners to uphold their rights without compromising personal data.

First, brand owners should map enforcement data. They should determine what is collected: screenshots, URLs, seller names, phone numbers, invoices, addresses, transaction records, platform communications, and investigation notes. Second, each category should be linked to a specific enforcement objective, including takedown, litigation, criminal complaint, customs enforcement, or monitoring repeat offenders.

Third, data minimisation should be implemented during the investigation phase. Screenshots should capture the infringing content and the seller's identifier, but efforts should be made to exclude irrelevant user comments or unrelated profile details. Fourth, takedown notices should be accurate and evidence-based. Fifth, access to enforcement files should be granted based on user roles and recorded in a log. Sixth, vendor agreements should include privacy and security obligations. Seventh, retention periods should be specified, and extended storage is allowed only in case of litigation, repeat infringement, or regulatory compliance. In the end, cross-border sharing should be reviewed and limited.

This model does not undermine brand enforcement. In fact, it enhances the credibility of enforcement. Courts and platforms are more inclined to take seriously detailed complaints, supported by evidence, and appropriately scaled. Consumers also benefit when counterfeit goods are removed without exposing unrelated personal data.

[17] Digital Personal Data Protection Act 2023

CONCLUSION

The DPDP Act marks an important shift in India's digital enforcement landscape. Brand owners are still fully empowered to monitor infringement, collect evidence, conduct test purchases, issue takedown notices or initiate legal proceedings. The Act expressly acknowledges processing connected with legal rights and the investigation of legal contraventions. However, it also requires enforcement to be necessary, secure, and accountable.

Therefore, the future of digital brand enforcement will depend on balance. Brand owners must protect goodwill, prevent consumer confusion and act against counterfeit goods. At the same time, they must avoid excessive data collection, insecure sharing and indefinite retention. Platforms need to address legitimate IP complaints while safeguarding seller and user data. Law firms and investigators must treat enforcement data as regulated information, rather than simply as commercial intelligence.

The DPDP Act does not treat privacy as conflicting with intellectual property. Both protect trust in the digital economy. Trademark law safeguards consumers and businesses against deception, whereas data protection law shields individuals from the misuse of personal information. A mature enforcement system must do both.