



India: courts adopt new ways to protect brand owners by permanent blocking of fraudulent domains and asset freezing

Thought Leadership • June 26, 2026

'First published on [WTR](#)'

By: [Saif Khan](#) and [Prajjwal Kushwaha](#)

Legal framework

Trademarks Act 1999

The Trademarks Act is the parent statutory regulation for trademarks in India. It provides protection of 10 years to several categories of marks, including buildings, shapes, sounds and collective marks, and recognises the rights of a prior and unregistered trademark user against a registered trademark. The term of protection can be extended by timely renewal applications.

Under the Act, a rights holder can pursue both civil and criminal remedies against an infringer. The Act also provides that an infringement suit can be instituted where the trademark owner actually and voluntarily resides or carries on business or personally works for gain. While the classification of goods and services under the Act is aligned with the Nice Classification, courts also apply provisions of the Act to protect the personality rights of public figures and celebrities.

Copyright Act 1957

The Copyright Act protects original literary, dramatic, musical and artistic works, as well as computer programs, films and sound recordings. While original literary, dramatic, musical and artistic works are protected for a period of 60 years following the death of the author, sound recordings, cinematographic films and photographs are protected for 60 years following the publication of the work.

The Act provides for the inalienable right of a rights holder to receive an equal share of royalty in the underlying work and bars the assignment of moral rights. It also penalises secondary infringement of



copyright – that is, acts that do not directly amount to infringement but facilitate infringement by others. Fair-dealing exceptions and grounds to initiate civil and criminal actions in infringement cases are also given in the Act. Like the Trademarks Act, the Copyright Act also creates an additional jurisdiction for the rights holder to initiate a suit where the holder actually and voluntarily resides or carries on business or personally works for gain.

Designs Act 2000

The subject matter protectable under the Designs Act extends to shapes, configurations, patterns, ornaments and compositions of lines or colours applied to any article in 2D or 3D form, or both, by any industrial process. The Act only protects only such non-functional aspects of a finished product that appeal when judged solely by the eye.

While the Act provides no criminal liability for design infringement, a rights holder can take civil action within the valid design protection period, which is an initial 10 years, extendable by a single five-year period. Any work capable of being registered under the Designs Act, when produced more than 50 times, automatically loses its protection under the Copyright Act.

Information Technology Act 2000

The Information Technology Act seeks to curb illegal infringing activities conducted through the use of computer systems and technology. With the growing deployment of IT infrastructure in e-commerce, supply chains and customer engagement, the Act's provisions have become more relevant than ever. The Act provides for the following offences:

- concealing, destroying or altering any computer source code or network;
- causing wrongful loss or damage to the public, or destroying, deleting or altering information in a computer resource or diminishing its value or utility;
- identity theft and cheating by impersonation;
- publishing obscene information in electronic form; and
- breaching confidentiality or privacy.

The setting up of dedicated cybercrime cells to investigate and prosecute offenders under the Act is evidence of the nation's policy against tech-enabled fraud.



INDRP

The .in Domain Name Dispute Resolution Policy (INDRP) is the framework for resolving disputes pertaining to any '.in' domain (India's country code top-level domain). Any person aggrieved by registration of a '.in' domain that is identical to or confusingly like their name or trademark may file a complaint before the National Internet Exchange of India (NIXI), which is the administrative body for addressing complaints under the INDRP.

Apart from the aforementioned statutes, the following regulations can also apply (depending on the facts and circumstances of each case):

- Geographical Indications Act 1999;
- Drugs and Cosmetics Act 1940;
- Food and Safety Standards Act 2006;
- Prevention of Money Laundering Act 2002;
- Data Protection Act 2023; and
- Consumer Protection (E-commerce) Rules 2020.

Border measures

The import of infringing goods is prohibited by the Customs Act 1962, read alongside the Intellectual Property Rights (Imported Goods) Enforcement Rules 2007. Seizures made by Pan-India Customs over the past few years offer important insights into the widespread influx of counterfeit goods and emphasise the critical need for strong enforcement measures at the border.

The law allows holders of specific IP rights – including trademarks, copyright, designs and GIs – to record their rights with Customs in order to secure the prompt seizure of counterfeit goods at the port of entry. The Act also prohibits the export of counterfeit goods, further strengthening the measures against counterfeiting. In order to get Customs to apprehend counterfeit goods intended for export, the rights holder must inform Customs about the shipment beforehand and in writing.

However, it is worth mentioning that for an effective Customs action, the rights holder is required to follow up and remain in constant communication with the authorities. Brands may further organise workshops and seminars to train and inform Customs authorities about the unique identifiers by which original and counterfeit products can be differentiated. Such activities will also motivate Customs to be more vigilant while scrutinising shipments.



Procedure under the Customs Act

Once IP rights are registered with Customs, the authorities can suspend the import of goods suspected to be counterfeit or infringing on their own initiative (where there are reasonable grounds to believe that the goods violate registered IP rights) or based on information provided by the rights holder. Customs will inform about the suspension of suspected counterfeit goods. Once the rights holder has confirmed that the goods are counterfeit, it must furnish a bond of an amount equivalent to 110% of the value of the detained goods along with security in the form of a bank guarantee or fixed deposit equivalent to 25% of the bond value. The value of the detained goods is determined based on the value of the goods declared by the importer.

Customs will then seize the suspended products and issue a show cause notice to the importer and all parties that facilitated the importation of the counterfeit goods, requiring them to explain why no action should be taken against them. Customs may also address the show cause notice to the rights holder, which should respond to assert its legal rights and confiscate the infringing goods, along with directions for destruction and penalty against the parties involved.

Before the matter is adjudicated by Customs, the importer and the rights holder have an opportunity to be heard before the adjudicating authority in person. After the hearing, Customs will pass an order for absolute confiscation and impose a penalty upon the importer and parties involved in importing the infringing goods. After the appeal period has expired, Customs will destroy the suspended goods. The rights holder must bear the cost of destruction, demurrage and detention. After the counterfeit goods are destroyed, the bond and bank guarantee are returned to the rights holder.

Criminal prosecution

Criminal remedies are provided under the Trademarks Act, the Copyright Act, the Geographical Indications Act and the IT Act. Under the extension of the Proceeds of Crime Act 2022 to IP matters, the assets of entities undertaking transactions while falsely using another party's IP may be seized by the authorities in addition to arrest.

Criminal offences under the Trademarks Act include the acts of falsifying and falsely applying trademarks and trade descriptions, as well as providing services to which false trademarks or trade descriptions are applied. Similarly, under the Copyright Act, knowingly infringing someone's copyright or dealing in infringing copies of computer programs are penal offences.

The 2012 amendments to the Copyright Act revolutionised India's copyright laws by amending its piracy laws. Section 65A of the Copyright Act protects technological protection measures (TPMs) used by copyright owners against any evasion or breach. If someone evades or circumvents a TPM in



order to infringe the owner's IP, then that person can be punished with a fine and imprisonment for up to two years.

Cases pertaining to offences under the Trademarks Act and Copyright Act are first lodged with the concerned police station. Upon registration, the raid action is conducted. The search and seizure cannot be conducted by an officer below the rank of deputy superintendent of police. This officer must seek the Trademarks Registrar's opinion before carrying out a search and seizure, which is one of the major issues that rights holders face when it comes to initiating criminal action against a counterfeiter. However, under the Criminal Procedure Code, the officer can seek a warrant from the court to conduct a raid under the Trademarks Act. In such situations, it is not necessary to get the registrar's opinion before the raid is conducted.

Effective criminal enforcement in India requires proactive liaison with the police both before and after filing the action. The complainant is required to assist the police at every stage of a criminal proceeding, which may be lengthy and time consuming. The practice of plea bargaining can save time in such cases, as the offender accepts guilt and the court imposes heavy costs payable to the rights holder.

The enactment of the Jan Vishwas (Amendment of Provisions) Act 2023 seeks to decriminalise certain offences under the Trademarks Act and Copyright Act. The key offences that have now been omitted or for which punishment has been diluted include falsification of entries in the register, falsely representing a trademark as registered and making false statements for the purpose of deceiving or influencing any authority or Copyright Office officer. However, specific provisions of the Jan Vishwas Act will come into force through the government's notification, with varied dates for domain-specific amendments.

Civil enforcement

All of the IP statutes provide for civil remedies in the form of injunctions and damages or rendition of accounts. A civil action is initiated by filing a lawsuit before the district court or high court that has territorial jurisdiction. Indian courts are well versed in IP laws, with the Delhi and Madras High Courts having dedicated IP divisions. Courts are becoming cognisant of the cross-territorial nature of online infringement and allow for suits to be filed before such courts where none of the parties have their offices, but where the infringer is providing its goods or services within the court's territory.

Several infringers can be joined in one proceeding, if a link can be shown between the entities. Links include if: (1) all the defendants are sourcing the products from the same supplier; (2) the counterfeit products have the same features; or (3) that the defendants are operating in the same market. Courts regularly grant ex parte interim injunctions, especially in such disputes where the impugned



product is a clear counterfeit.

Rights holders can obtain the following interim reliefs in civil actions:

- Anton Piller orders – the rights holder may seek ex parte appointment of court commissioners to visit the defendant's premises to find and seize counterfeit goods. The goods are returned to the defendant with an undertaking that they will be safely preserved until further court orders.
- John Doe orders – this is an extraordinary order, through which the court can appoint court commissioners and authorise them to enter, search and execute seizures in the premises of any named or unnamed defendants. This kind of action is most effective where it is difficult to identify every counterfeiter or the counterfeiter is operating out of temporary premises.
- Mareva injunctions – in specific cases an injunction may be granted against infringers to freeze their assets until further court orders.

IP disputes qualify as commercial suits under the new system for commercial cases. This provides expedited timelines for each stage in a civil case. In the event that in an ongoing civil suit the defendants fail to appear or raise a plausible defence in their initial pleadings, an application for summary judgment can be moved. In such cases, courts can decide the matter finally without requiring oral evidence to be heard.

By their very nature, anti-counterfeit lawsuits are fit for invoking summary proceedings – especially after the successful execution of an Anton Piller order.

Mediation is also a viable option for trademark owners, and Indian courts often encourage this in IP disputes. By opting for mediation, not only can one secure an upfront amount as damages, but settlement by way of mediation also entitles the plaintiff to a full refund of the government court fees submitted for instituting the case.

Domain names

Indian courts faced a disturbing pattern of cyber fraud where unknown individuals registered domain names incorporating the well-known trademarks. These fraudulent domain names were being systematically exploited to deceive innocent members of the public through various schemes, including fake job offers and franchise opportunities, and distributorship schemes. The *modus operandi* was particularly insidious: registrants would create websites hosting almost identical content to the brand's official website, use similar logos and marks, and provide misleading information to entice the public into making payments through digital transactions to bank accounts completely unconnected to the brand. The gravity of the situation was compounded by the fact that the WHOIS details of infringing domain names were systematically masked by domain name registrars (DNRs) using "privacy protect" features, preventing plaintiffs from initiating proceedings

India: courts adopt new ways to protect brand owners by permanent blocking of fraudulent domains and asset freezing



against the actual perpetrators.

The Delhi High Court heard a batch of these matters together and recognised that these were not isolated incidents but systemic problems requiring consolidated investigation and comprehensive remedies. Investigation by the Intellectual Fusion and Strategic Operations unit of the Delhi Police revealed that crores of rupees had been fraudulently collected from innocent individuals duped by these infringing domain names. The scale of the fraud was staggering, with status reports indicating illegal collection of substantial amounts under the garb of offering distributorships, franchises and employment. The court heard relevant stakeholders at length and passed comprehensive directions to address the systemic failures.

Directions to DNRs and registry operators

The court held that DNRs shall not mask details of registrants on a default "opt-out" basis; privacy protection should only be provided if specifically chosen by the registrant. All DNRs enabling registration of domain names administered by NIXI must provide requisite registration data to NIXI within one month. DNRs must appoint grievance officers, and service by email to these officers shall constitute sufficient service for court orders. DNRs that insist on a mutual legal assistance treaty or other modes of service shall be held noncompliant.

Directions to government authorities

The court directed the government to hold stakeholder consultations with DNRs and registry operators to explore a framework similar to that used by NIXI. The government must consider nominating NIXI as a data repository agency for India, with which all registry operators and DNRs would maintain registrant details on a periodic basis, or alternatively, DNRs shall localise data in India. Most significantly, the court held that noncompliant DNRs or registry operators may be blocked by the Ministry of Electronics and Information Technology and the Department of Telecommunications of New Delhi under section 69A of the IT Act.

Banking sector reforms

The judgment addressed crucial gaps in the banking system that facilitated fraud. The court noted that fraudsters could receive payments because innocent people did not realise they were not paying the actual brand owners. Pursuant to court directions, the Reserve Bank of India introduced the Beneficiary Bank Account Name Lookup facility for Real Time Growth Settlement and National Electronic Funds Transfer systems on 30 December 2024. This allows remitters to verify the name of the bank account to which money is being transferred before initiating the transfer, thereby preventing mistakes and fraud. All banks were mandated to implement this facility without any charge to customers by 1 April 2025. The court also directed all banks to abide by the standard operating procedures issued by the Central Economic Intelligence Bureau for processing and



responding to requests from law enforcement agencies.

Bank account freezing

In cases of clear and large-scale counterfeiting, Indian courts are granting ex parte Mareva injunctions when it is satisfied that there is a prima facie case of infringement supported by documentary evidence and a clear link between infringing sales and the bank accounts established through invoices and complaints from consumers.

In such cases, courts adopt “a balanced and a proportionate approach” by recognising that freezing accounts may impair business operations. Hence, the courts are also granting directions to banks for filing of statements, disclosure of full KYC details and filling of details in sealed cover judicial inspection. This measure allows preservation of the disputed funds without hampering the defendants’ lawful operations.

This approach is appropriate for maintaining status quo concerning the proceeds in the accounts generated through alleged infringement. This trend reinforces proper use of interim injunctions, especially in counterfeiting cases, in which sale proceeds are often the recoverable evidence.

Anti-counterfeiting online

The success of e-commerce businesses in India has allowed illegal operators to conveniently sell counterfeit products under the guise of heavy discounts and a shield of anonymity that is otherwise unavailable for original products. No distinction is made between online and offline counterfeiting and no law is in place that deals specifically with online counterfeiting. However, the IT Act specifically provides for the liability of Internet intermediaries.

In a recent case involving an e-commerce marketplace, the court observed that such marketplaces cannot become havens for counterfeiters. It noted that the platform had facilitated counterfeiting by allowing such listings to be put on its platform without verifying the sellers of such listings. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 also require online platforms to put mechanisms in place that proactively identify infringing content. Failure to comply with this requirement may lead to intermediaries losing the safe harbour protection.



Smart copying and latching on: evolving challenges in IP enforcement

Smart copying represents a sophisticated form of IP infringement where the copier deliberately incorporates key elements of a protected work while making superficial changes to avoid exact duplication. This practice was highlighted in a recent case where the court found significant similarities in the overall appearance, including ribbon-like features, colour schemes and placement of elements, concluding it was “a clear attempt at smart copying”. Such copying is particularly problematic in fast-moving consumer goods, for example, where consumers may not get adequate time or opportunity to easily distinguish between products, leading to confusion about product origin or affiliation.

Similarly, “latching on” presents another emerging challenge in the digital marketplace, particularly on e-commerce platforms. This practice allows sellers to link their products to successful listings of other sellers, potentially riding on established goodwill. Whether latching on constitutes passing off, courts take different views and a clear determination is awaited. While some judgments find latching on to be “riding piggyback” and “taking unfair advantage of goodwill”, others suggest that merely providing links to competing sellers does not inherently constitute passing off. The key consideration appears to be whether the latching-on seller misrepresents its products as emanating from the original seller, particularly through use of the original seller's brand name, logo or product images.

Online strategies

Online counterfeiting requires a sophisticated investigation strategy, which may include a combination of online surveillance using high-tech tools, personal visits and physical relative analysis of the products. Further, tackling online counterfeiting requires identification of the most effective targets along the chain, including website owners, domain hosts, Internet service providers (ISPs) and payment gateways.

Intermediary liability

The IT Act outlines the liability of Internet intermediaries – including entities such as ISPs, hosts, search engines, online payment sites, auction sites, marketplaces and cyber cafes – within its definition. While intermediary liability is subject to certain exemptions, adherence to the due diligence requirements specified by law is crucial.



With the surge in online counterfeiting, particularly through marketplaces, legal actions involving the responsibilities of intermediaries have risen. These intermediaries may include domain registrants, online marketplaces and call centres, among others. Courts are increasingly holding intermediaries to stricter standards and issuing injunction orders, in recognition of their active involvement in infringement and the substantial revenue generated by such activities.

Cybersecurity and brand protection

Recent trends show that cybersecurity and brand protection go hand in hand. This is particularly evident in cases of tech support fraud and call centre scams. Individuals posing as certified technical experts from reputable IT companies deceive victims into believing their systems are infected, offering to fix the issue for a fee. The fraudulent transactions appear authentic as the pop-ups vanish, convincing users of a genuine threat. Several affected brand owners have taken legal action, resulting in police raids uncovering significant fraudulent transactions and leading to numerous arrests.

Preventive measures/strategies

Ascertaining and handling confidential information

While one strategy may not fit well for all types of anti-counterfeiting efforts, a common element of maintaining confidentiality applies across the board. The particulars of the infringer, its premises and the number of people employed must be ascertained beforehand, as it is only upon receiving such information that the court will grant the reliefs sought once it is satisfied that the defendant is indeed a counterfeiter.

Reconnaissance must be conducted right before executing an Anton Piller order in order to efficiently allocate resources and plan the raid action. Raids may have to take place at multiple locations. To ensure the information about the raid is not leaked and the infringing goods are not removed, teams must coordinate with one another and start the raid action simultaneously.

Safe and legal execution of Anton Piller orders

It should be ensured that the legitimate business operations of the defendant are not disturbed while executing the raid action and only the infringing goods are sealed. Raid actions can involve unforeseen circumstances, such as nuisance by the infringer or interference by market entities. To avoid any mishap, civil raids must be conducted after obtaining the necessary protection from local law enforcement. The entire exercise must be properly photographed or videoed, and an on-the-



spot proceeding must be prepared that should be duly signed by everyone present.

Effective use of anti-counterfeiting features

Brand owners can deploy several preventive technologies to identify genuine products and ensure a tamper-proof supply chain. Microscopic tags, barcoding, licence databases, unique identity codes or holograms, and seals of authenticity can all prevent the proliferation of counterfeit and pirated products.

Brands are exploring various uses of blockchain technology to combat counterfeit products in the market. A unique identifier or a digital token, which is linked to a blockchain, can provide instant verification of the product's description and the entities involved in the supply chain.

Partnership between public and private stakeholders

Industry leaders must join together to devise practical and tailored solutions to combat counterfeiting in their respective industries. Recent collaborations between global tech giants and central investigation agencies have proved fruitful in uncovering large-scale cyber hubs that were engaged in defrauding customers through impersonation. Similar collaborations are required from industry-specific stakeholders, and a targeted approach is required to create market impact by catching the key players in counterfeit supply chains.



KEY CONTACT



Saif Khan

Partner

[View Bio of Saif Khan](#)