India: lack of court harmonisation in tackling emerging online infringement threats underscores need for further case law

Thought Leadership • June 28, 2025

'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 right 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, provisions of the Act are also applied by courts 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, cinematograph films and photographs are protected for 60 years following the publication of the work.

The Act provides for the inalienable right of a right holder to receive an equal share of royalty in the underlying work and bars the assignment of moral rights. The Act 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 right 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 2- or 3-dimensional 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, civil actions can be taken by a right holder within the valid design protection period, that is, an initial 10 years, extendable by a single 5-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 (IT) 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 before. The Act provides publishment 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.
- 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.

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 (ie, the country code top-level domain for India). 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, which is the administrative body for entertaining complaints under the INDRP.

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

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 borders.

The law allows holders of specific IP rights – including trademarks, copyright, designs and geographical indications – 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 right holder must inform the Customs about the shipment beforehand and in writing.

However, it is worth mentioning that for an effective Customs action, the right 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 right holder. Customs will inform about the suspension of suspected counterfeit goods. Once the right holder has confirmed that the goods are counterfeit, they 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.

Thereafter, Customs will seize the suspended products and issue a show cause notice to the importer and all parties that facilitated the importation of counterfeit goods, requiring them to explain why no action should be taken against them. Customs may also address the show cause notice to the right holder, who should respond to assert their 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 right 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 cost of destruction, demurrage and detention must be borne by the right holder. After the counterfeit goods are destroyed, the bond and bank guarantee are returned to the right 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 Law to IP matters, the assets of entities undertaking transactions while falsely using another party's intellectual property 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, trade description and so on, and providing services to which false trademark or false trade description is applied. Similarly, under the Copyright Act, knowingly infringing someone's copyright or knowingly dealing in infringing copies of computer programs are penal offences.

The amendments to the Copyright Act in 2012 revolutionised India's copyright laws by amending its piracy laws. Section 65A of the Copyright Act protects Technological Protection Measures (TPM) 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 imprisonment for up to 2 years along with a fine.

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 must be conducted by an officer not below the rank of Deputy Superintendent of Police. This officer must seek the opinion of the Registrar of the Trademark before carrying out a search and seizure. This is one of the major issues faced by rights holders in initiating criminal action against a counterfeiter. However, under the Criminal Procedure Code, the officer can seek warrants from the court to conduct a raid action under the Trademarks Act. In such situations, it is not necessary to get the opinion of the registrar before the raid action 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 the guilt and the court may impose a fine on the accused and award compensation payable to the rights holder.

The recent 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 which 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 officer of the Copyright Office. However, specific provisions of the Jan Vishwas Act will come into force through Central 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 High Court of Delhi and Madras having a dedicated IP Division. 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 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; that is, that all the defendants are sourcing the products from the same supplier, that the counterfeit products have the same features or 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 in order to find and seize counterfeit goods. The goods are returned to the defendant with an undertaking that they will be safely preserved until further orders of the court.
- 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 where the counterfeiter is operating out of temporary premises.
- Mareva injunctions: in specific cases, an injunction may be granted against the 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 do not enter an appearance or raise no 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 have seen a sharp rise in new cases of fraudulent domain name registration. A right holder can seek an injunction for the interim and permanent takedown or transfer of the domain name in a civil lawsuit. As in most cases, the name and details of the domain registrants are masked, a right holder can also request the details of the registrant as well as the details of the bank account used to purchase the fraudulent domain.

Fraudulent domain names help online counterfeiting as they allow infringers to lure bona fide customers into placing orders, who in return get counterfeit products or no product at all. The diversion of traffic away from the original website or platform has become a major problem for brands. Common tactics deployed to divert traffic include opening fake social media accounts, purchasing ad-words containing trademarks of the original brand to rank the impersonating website higher in the search results and using meta-tags in the source codes.

Courts are now actively enquiring into non-compliances by intermediaries and digital platforms, such as the non-appointment of grievance officers and loose know-your-customer policies followed by domain name registrars, banks, telecom operators and other entities. Without such credible information, it is difficult for victims and brand owners to ascertain the identity of the real fraudsters.

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 there is no law 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. The court 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 intellectual property 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, for example, the fast-moving consumer goods industry, where consumers in may not be 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 the established goodwill of original sellers. Whether latching on constitutes passing off or not, there are different views taken by court 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 doesn't inherently constitute passing off. The key consideration appears to be whether the latching-on seller misrepresents their 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 and 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, their 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/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.

Various uses of blockchain technology are explored by brands 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 of 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