Marketplace liability 2.0: when does an e-commerce platform become a trademark infringer?

Thought Leadership • April 28, 2026

First published by The Trademark Lawyer

Written by Lakshmidevi Somanath

Not long ago, platform liability for trademark infringement was a minor concern. The major e-commerce marketplaces had successfully positioned themselves as neutral entities, and brand owners had accepted a world of takedown notices. Now the passive intermediary model that sheltered platforms for nearly two decades has run its course, and the debate has shifted from whether platforms bear any responsibility for infringement on their systems to how much, and on what terms.

Counterfeiting accounts for $467 billion in global trade annually, according to the OECD's 2025 figures, and e-commerce platforms have become its dominant distribution channel. Even if a very small fraction of product listings are infringing, the sheer volume of counterfeit goods reaching consumers is enormous. The question is whether the platforms can finally be required to share the burden of it.

USA – from *Inwood* to the digital marketplace

The foundational doctrine goes back to *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.* (1982), where the Supreme Court held that a party could be contributorily liable for trademark infringement if it either intentionally induced another to infringe, or kept supplying goods or services to someone it knew, or had reason to know, was infringing. It was a sensible test, but it was designed for manufacturers supplying physical products, not for companies running digital platforms with tens of millions of anonymous third-party sellers.

When Tiffany sued eBay in 2010, the Second Circuit had to apply those principles to the internet for the first time. The result was highly favorable to platforms. Liability required notice of specific, identified infringements, and generalized awareness that counterfeiting was rampant on the platform was not enough. In practice, this meant a platform could largely immunize itself from contributory liability by processing takedown notices efficiently, without doing anything about the

structural conditions that made those infringements so persistent. Based on these platforms, takedown portals, and brand owners built monitoring teams. However, the system was imperfect since infringers simply reregistered under new storefronts after being removed.

The Ninth Circuit's 2023 decision in *Y.Y.G.M. SA v. Redbubble* threw into relief how awkward the *Tiffany* doctrine had become in a world where platforms run sophisticated algorithmic advertising, earn commissions on every transaction, and are, in many product categories, well aware that counterfeiting is endemic.

The case that brought the tension into the open most sharply was *Kelly Toys Holdings, LLC v. 19885566 Store*, which centered on counterfeit Squishmallow toys sold through Alibaba and AliExpress storefronts. In June 2023, the Southern District of New York held Alibaba in contempt for aiding merchants who were subject to an injunction against selling counterfeit goods. Alibaba actively marketed counterfeit products through sponsored ads and promotional emails and continued providing premium merchant services to sellers it knew were enjoined. That is not passive hosting. The contempt order was partially vacated on reconsideration, but the underlying contributory infringement claims survived Alibaba's motion to dismiss, and the case makes clear that a platform actively monetizing infringing activity cannot fall back on *Tiffany v. eBay* as a complete shield.

What the American cases as a whole illustrate is that the doctrine is alive and moving, even if it progresses slowly. The willful blindness standard means that a platform that suspects widespread counterfeiting in a category and deliberately refrains from investigating cannot later claim it lacked specific knowledge. The Eleventh Circuit's 2019 decision in *Luxottica Group, S.p.A. v. Airport Mini Mall* is worth recalling here, even though it involved a physical mall rather than a digital marketplace. The court affirmed contributory liability against a landlord who had received police raids and written notices, yet did nothing. The principle translates: an infrastructure provider that profits from an infringer's presence and takes no meaningful action is exposed, whether the infrastructure is bricks or code.

Europe – the Digital Services Act and its IP implications

The Digital Services Act, fully in force since 2024, is the most significant change to online intermediary liability in the EU since the E-Commerce Directive of 2000, and its consequences for trademark enforcement are still working their way through the system.

The DSA does not replace the notice-and-respond model, but it layers obligations on top of it that fundamentally change what compliance means. Very Large Online Platforms (VLOPs), those with more than 45 million monthly active users in the EU, face the heaviest requirements. They must

conduct annual systemic risk assessments covering the spread of illegal content, a category that includes counterfeit goods, implement documented mitigation measures, submit to independent audits, and appoint compliance officers accountable to national Digital Services Coordinators. Non-compliance can mean fines of up to 6% of global annual turnover, or in serious cases, suspension from the EU market.

Amazon, Alibaba, and AliExpress all qualify as VLOPs. Each must now demonstrate, through formal risk assessments and audit trails, how it identifies and addresses IP infringement risks on its platform. That is categorically different from responding to individual complaints. It is an obligation of structural vigilance, not reactive administration.

In December 2025, the Commission issued its first major DSA enforcement decision, a €120 million fine against X (formerly Twitter) for transparency violations. The Commission also signed an agreement with the European Union Intellectual Property Office in 2025 specifically to reinforce IP enforcement under the DSA, creating an institutional link between two bodies that had previously been operating in parallel.

AliExpress became the subject of formal DSA investigations in June 2025, focused on user and consumer safety. Temu faced formal proceedings from October 2024. Temu's regulatory problems also extend beyond Europe: it was separately required to pay $2 million for violations of the US INFORM Consumers Act, and removed 1.2 million listings for IP violations in 2025 under its own Brand Protection Policy. Independent investigators found that its AI moderation system catches around 68% of infringing listings within 48 hours, which sounds reasonable until you consider that the remaining third stay live for an average of nearly 12 days. For brands fighting active counterfeiting campaigns, that gap is a real problem.

The DSA's two-tier enforcement structure is worth understanding in practical terms. The Commission handles VLOPs directly. National Digital Services Coordinators handle smaller platforms in their member states. A brand owner pursuing counterfeits across platforms of different sizes may find itself navigating Commission-level processes and national regulatory procedures at the same time, potentially in multiple member states. It is manageable, but it requires planning rather than improvisation.

The broader contrast with the US Section 230 framework also matters. Section 230 offers platforms broad immunity with narrow exceptions. The DSA provides a conditional exemption that requires ongoing compliance with specific obligations as the price of protection. A legal strategy built around US common law principles will not translate cleanly to a European regulatory context, and brand owners with significant European exposure need to understand that.

The Asia-Pacific dimension

The legal framework in India is Section 79 of the Information Technology Act 2000. It grants safe harbor to platforms operating as neutral intermediaries that observe due diligence. However, it removes it where a platform conspires, abets, or actively facilitates unlawful conduct. In *Christian Louboutin SAS v. Nakul Bajaj & Ors* (2018), the Delhi High Court mapped out 26 specific activities that could, taken together, push a platform across the line from passive conduit to active participant and place it outside the Section 79 exemption. In *Amway India Enterprises v. 1MG Technologies* (2019), it was held that platforms providing warehousing, fulfillment, and other value-added services had become too involved in the transaction to claim the safe harbor provision. On appeal, the division bench subsequently held that offering additional services does not, on its own, forfeit safe harbor protection. In *IndiaMART Intermesh Ltd. v. PUMA SE.* (2024) it was held that IndiaMART's use of the PUMA trademark in its seller registration drop-down menu amounted to infringement and that the platform was aiding and abetting counterfeiting, denying it safe harbor altogether. On appeal, the Division Bench characterized IndiaMART as closer to a listing directory than a transactional marketplace, finding no dishonest intent in the drop-down feature, and restoring safe harbor protection subject to a clear obligation to remove infringing listings promptly once notified. What emerges from the case law is a liability threshold broadly consistent with the US position after *Tiffany v. eBay.* There is no express provision in the Trade Marks Act 1999 addressing platform liability in digital marketplaces.

China's E-Commerce Law, in force since 2019, Article 38 imposes joint and several liability on platform operators where they knew or should have known of infringement and failed to take necessary measures. is explicit about this. This aligns with a European-style standard of platform accountability.

China's State Administration for Market Regulation ('SAMR') investigated 27,000 IP-related cases in the first nine months of 2024, involving illicit gains of 468 million RMB and producing 742 criminal referrals. But they coexist with a structural problem of ghost storefronts. A targeted crackdown on just 14 stores across Pinduoduo, Taobao, Kuaishou, and JD.com found that 10 were registered at nonexistent addresses and 8 were completely untraceable. This points to a systemic gap between what the law says and what enforcement can actually reach.

SAMR began drafting revised regulations in October 2024 with that gap in mind. As per this, platforms would need to verify seller identity details and keep them accurate. They would have five working days to act on notifications of suspected infringement. More notably, the draft proposes real-time integration with public IP databases, so that if a trademark is canceled, opposed, or reassigned, the platform automatically suspends linked listings within 48 hours.

Alibaba has invested heavily in its Intellectual Property Protection Platform, which consolidates

enforcement across Taobao, Tmall, Tmall Global, AliExpress, and Lazada. It handles more than ten million notices a year, covering trademark, copyright, and patent complaints. Since 2016, Alibaba has also brought its own civil actions against counterfeit vendors. The Taobao three-strikes policy for repeat offenders, introduced in 2017, reflects a genuine understanding that removing listings is not enough if the same sellers just come back.

However, takedown requests on Taobao and Tmall require Chinese-registered rights. A foreign brand without a Chinese trademark registration simply has very limited tools on those platforms, regardless of what it holds at home. It means any brand with serious exposure to Chinese e-commerce has to treat a Chinese trademark registration as a basic commercial requirement.

Japan, South Korea, Australia, and Singapore each have their own platform liability frameworks. In Southeast Asia, several of the most commercially significant markets are still developing their positions.

Passive infrastructure or active participant?

Are these platforms passive carriers, more like a postal service than a retailer, with no meaningful responsibility for what moves through their systems? Or are they active commercial participants who profit from every transaction and should bear some of the consequences when those transactions involve infringing goods? The US, EU, and China have reached different provisional conclusions, and those differences account for most of the divergence in liability outcomes.

The case for the passive intermediary view is straightforward. Amazon does not choose or manufacture the goods its third-party sellers list. No platform could realistically review hundreds of millions of listings for IP compliance before they go live. Imposing proactive monitoring at that scale would create unworkable burdens and would fall disproportionately on the small businesses that depend on marketplace access. Platforms do provide enforcement tools such as Brand Registry on Amazon, the IPP Platform on Alibaba, and VeRO on eBay. Those mechanisms work even if they require the rights holder to do most of the investigation.

The counter-argument is that these platforms sell advertising to sellers, and there is documented evidence that this advertising has gone to sellers of counterfeit goods. They take commissions on every transaction, infringing or not. They provide fulfillment and logistics. They run recommendation algorithms that surface products based on commercial criteria with no relationship to IP status. When a genuine product and its counterfeit competitor appear side by side in the same search results, the platform earns from both. Therefore, they cannot be said to be neutral.

The DSA's systemic risk assessment requirement signals that European legislators have reached a similar conclusion. Platforms at sufficient scale are no longer permitted to describe themselves as

neutral pipes. They must assess what their systems actually produce and show that they have addressed the risks. That marks a real shift, and it will take years for its full implications to become clear.

The small-parcel problem and cross-border enforcement

Earlier waves of counterfeit goods moved in large commercial shipments that could be intercepted at ports of entry. Customs recordation was a practical deterrent. That model has been largely displaced, at least for these platforms, by direct-to-consumer shipping of individual parcels, each designed to fall below the de minimis customs threshold. A 2023 report by the US House Select Committee on Strategic Competition identified the exploitation of this loophole as a key mechanism through which platforms avoid customs scrutiny. The result is that infringing goods routinely reach consumers before a rights holder has any realistic opportunity to intercept them.

Border seizures and customs recordation still have value, but they are not scaled for a world where millions of small packages move daily through postal channels. By the time notice arrives of a specific infringing shipment, it is often already delivered. The only tool that operates at the relevant scale is platform-level enforcement. If you cannot intercept the parcels, you have to go after the platform conditions that produce them.

This is part of why the DSA's systemic risk framework has drawn real interest from IP practitioners working in the EU. A platform processing millions of direct-to-consumer shipments of potentially infringing goods cannot credibly claim it has no awareness of the risk. Showing that a VLOP failed to conduct adequate risk assessments or failed to implement proportionate mitigation is a more workable enforcement path than establishing specific knowledge of specific listings. In the US, the courts will have to develop this argument through litigation, and the doctrine is still catching up. But the direction of travel is consistent with where Europe has already arrived.

What brand owners should actually do

Given the state of play across these jurisdictions, effective enforcement needs to be treated as a strategic function, not an administrative one.

Multi-jurisdictional trademark registration has moved from good practice to a condition of enforcement. Alibaba's IPP Platform requires Chinese-registered rights for takedown requests on Taobao and Tmall. DSA mechanisms work only on the basis of rights valid in the EU. A brand owner whose registrations are concentrated in its home jurisdiction will find itself without meaningful tools on the very platforms where infringement is most active. The cost of filing in China, the EU, the UK,

Japan, and Australia is a fraction of what brands spend dealing with infringement in those markets without proper coverage.

Building an evidence record around the platform's actual knowledge and conduct has become genuinely important, not just as a litigation precaution but as a strategic asset. The *Kelly Toys* litigation showed what happens when a rights holder can demonstrate that a platform did not merely fail to act quickly enough, but actively promoted infringing goods through sponsored ads and email campaigns while continuing to serve premium accounts it knew to be subject to an injunction. Rights holders should be capturing not just the infringing listings, but the surrounding commercial context: the advertising the platform ran for those sellers, the services it provided, and the notices it received. That is the evidence base that shifts a case from a takedown dispute to a platform liability claim.

The DSA has created enforcement pathways that simply did not exist before. The Commission's partnership with EUIPO means that documented evidence of systemic IP infringement on a VLOP can be brought before a regulatory body with real enforcement powers, not just submitted through a platform's private takedown interface. National Digital Services Coordinators add a further layer. These mechanisms are still new, and their practical reach is not yet fully established, but they represent a genuine addition to the toolkit for rights holders operating in Europe.

In China, the SAMR draft regulations deserve close attention. Brand owners relying primarily on Alibaba's IPP Platform should recognize that a more mandatory framework for platform conduct is in development. If it comes into force broadly as drafted, it would give rights holders a stronger footing in individual enforcement actions and potentially reduce the volume of infringement they need to manage reactively.

More broadly, the narrative that platforms bear no responsibility for the commercial conditions on their systems deserves to be challenged. Notice-and-takedown made sense when platforms genuinely lacked the technical means to do more. That is not the world we are in today. Platforms capable of running real-time personalized advertising and AI-powered recommendation engines are not helpless in the face of counterfeiting. European law has recognized this. US doctrine is moving toward the same conclusion, if more slowly. Rights holders who press these arguments now, rather than waiting for the law to fully settle, will be better placed when it does.

Conclusion

Earlier, a brand owner pursuing platform-level liability faced a passive intermediary model, with enforcement options that were limited to notice-and-takedown and then litigation. Now the DSA has introduced a structural accountability framework in Europe. US courts have affirmed that platforms

that cross from passive hosting into active commercial participation in infringement are exposed. India has expanded the scope of intermediary liability. China is tightening its mandatory platform obligations. These developments are not happening in coordination, but they are pointing in the same direction.

Platforms have significant commercial incentives to avoid serious liability exposure, and the legal tools to create that exposure are improving. Rights holders who understand are better placed than those who do not.

KEY CONTACT

Lakshmidevi Somanath

Partner

View Bio of Lakshmidevi Somanath