Protecting IP in the AI Era: Automation and Volume Are Reshaping Enforcement Strategy

Intellectual property (IP) enforcement has historically moved in sequence. A counterfeit product appeared, a copied logo surfaced or a pirated file circulated, and the original owner would contact a lawyer, who'd investigate and file a lawsuit. But that model is beginning to shift.

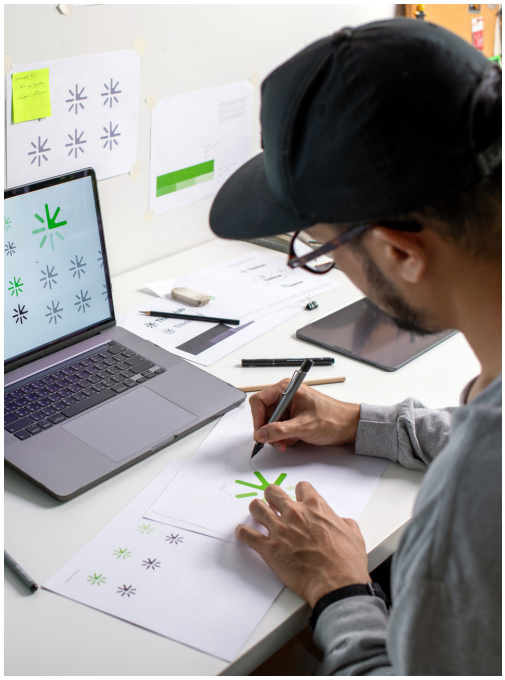
Artificial intelligence (AI) has fundamentally changed how infringement occurs and how it's defended. Coupled with digital marketplaces and global distribution, AI multiplies infringement risks. Copying is nearly instantaneous and harder to identify. Distribution is borderless. The number of violations can easily grow exponentially overnight.

The sheer scale of infringement has changed so dramatically that traditional IP litigation and manual review processes no longer keep pace, according to CEB technology law reporter Alexis Keenan, who covered the issue at the global **Web Summit in Lisbon**.

"The pace and rate of infringement has reached a level that simply cannot be managed by human lawyers alone," Keenan said.

AI now plays a dual, contradictory role in the marketplace. It consumes protected works to train models and can produce content that facilitates copyright infringement within seconds. At the same time, AI can help monitor, detect and enforce IP rights.

In the AI era, a modern IP enforcement strategy looks less like litigation and more like logistics.



"The pace and rate of infringement has reached a level that simply cannot be managed by human lawyers alone,"

The escalating scale of IP infringement

The numbers tell the story.

Before generative AI became mainstream, U.S. officials in 2017 estimated the national economy was losing an estimated **$225 billion to $600 billion annually to IP theft**, mostly due to violations by Chinese actors. Now, global trade in counterfeit goods alone is projected to reach **$1.79 trillion by 2030**, a 75% increase from 2023. By the end of the decade, as much as $1 out of every $20 spent worldwide could go toward counterfeit products.

Layer rapidly produced AI-generated listings on top of that, and enforcement challenges could escalate. Infringing listings can be generated automatically. Brand knockoffs appear on digital marketplaces within days, sometimes hours, of a product launch. Digital content can be scraped, altered and reposted across thousands of sites simultaneously. By simply flipping an image or video, AI can make copied images and videos difficult to track. Using someone else's IP has become cheap and scalable.

However, the same technology can also be used to detect, monitor and enforce. In an interview with Keenan, international IP attorney Rytis Rudzinskas and technology entrepreneur Thomas Eriksson described AI as a "sword and a shield" for IP. Rudzinskas represents rights holders in U.S. and European courts, while Eriksson founded the digital image-detection software, **Sasha SafeShare**.

The sword: tools that enable copying, scraping and replication at unprecedented speed and volume.

The shield: tools that help rights holders and attorneys detect infringement across marketplaces, social platforms and websites and automate enforcement actions.

Unfortunately, the sword works faster than traditional legal responses can protect rights holders. Managing AI-assisted infringements on a case-by-case basis is impossible in a world of dozens to thousands of violations per week. Instead, enforcement requires continuous monitoring and automated reporting systems anchored by a repeatable takedown strategy.

By the end of the decade, as much as

$1 out of every $20

spent worldwide could go toward counterfeit products.

The operational shift in enforcement strategy

For years, IP enforcement strategy has focused on significant disputes involving a major counterfeit ring, rogue distributor or competitor misusing trade secrets. Litigation was sporadic and defendant-focused.

Now, IP violations are often committed by anonymous sellers and operators of short-lived digital storefronts and overseas operations that rapidly respawn websites and scrape or remix digital content. By the time a complaint is filed, the infringer may have disappeared or relaunched under a new name.

Highly effective platform monitoring and automated legal filing systems could be enough to deter bad actors — and practitioners and their clients out of court. However, technology's success in catching IP infringement will depend on detection, speed, documentation and lawyers' workflow discipline.

Automated enforcement frameworks are expected to cause a spike in:

- Takedown notices
- Platform escalations
- Customs and border actions
- Coordinated cross-border enforcement
- Out-of-court enforcement

The cross-border challenge

The borderless digital world is also exacerbating IP theft, as infringers often operate across multiple jurisdictions and use shell entities to remain anonymous. This makes attribution difficult and expensive. Even when a defendant can be identified, jurisdictional hurdles could make pursuing litigation abroad impractical.

As a result, cross-border enforcement often shifts toward requesting takedowns from intermediaries, such as online retailers, like U.S.-based Amazon, Walmart and eBay, China-based Alibaba, JD.com, Shein and Temu, and Japan-based Rakuten, or hosting providers, payment processors or logistics networks.

This raises new questions around liability. Who should be responsible for preventing counterfeit listings, especially when digital retailers may not be incentivized to take down allegedly offending products? Removing listings can reduce a platform's revenue or create administrative costs. Without stronger platform liability standards or regulatory pressures, many platforms may be less likely to protect rights holders.

For IP lawyers, the new reality requires broader coordination and a more strategic approach to a client's pressure points beyond traditional legal claims. At the same time, policy remains unsettled, leaving practitioners to operate without clear guardrails.

Policy and regulatory framework

As with most technological advancements, the legal framework surrounding AI and IP is still catching up. At the center of the debate is whether AI-fueled technologies truly create new value when they rely on proprietary works to generate output or merely redistribute the original creator's content. That distinction will influence judicial and regulatory decisions on the extent to which proprietary works can be used to train AI systems, as well as the damages and enforcement costs associated with the misuse of rights holders' works.

If courts or regulators adopt the view that the technologies merely transfer value or benefit from copyrighted material without adding anything new, it would be a boon for creators. Licensing requirements would likely follow and statutory damages could increase. Platforms, in that case, could face stronger obligations to prevent infringement, and in turn, enforcement actions could become more financially viable for rights holders.

On the other hand, if judges or regulators characterize AI outputs that rely on original works as "transformative" and as value-creating, the burden may fall more heavily on creators and their counsel. Courts would foreseeably be reluctant to restrict training practices and require that AI systems license original works, and private enforcement could become more expensive and uncertain.

Early litigation signals just how unsettled the landscape remains. In one of the largest copyright settlements to date, Anthropic agreed to pay **$1.5 billion** to resolve claims from a group of authors alleging that it illegally trained its chatbot Claude using an online pirated library containing seven million copyrighted books. Before the settlement, the judge had ruled that Anthropic would have to face the authors' claims of copyright infringement.

At the same time, several courts have suggested that certain AI training on copyrighted material may qualify as fair use, depending on how the content was obtained and whether the model's outputs compete with the original works. For now, the few rulings and lack of regulation create a patchwork of unclear guidelines.

States are beginning to respond. California advanced AI transparency and reporting measures intended to increase accountability for how AI systems are built and deployed, with several **new laws taking effect in 2026**.

At the federal level, House lawmakers recently proposed new transparency requirements in the **Transparency and Responsibility for Artificial Intelligence Networks (TRAIN) Act**. The bill would allow copyright holders to use an administrative subpoena process to determine whether their works were used to train AI models and to obtain copies of relevant training records. If enacted, the measure would give creators a discovery tool to track how their content is used.

While courts and regulators are still drawing the lines, waiting for clarity is not a practical strategy.

The IP lawyers playbook

Until that clarity arrives, IP litigators need practical systems that they can implement.

Attorneys say that traditional, core advice to clients on protecting their IP should remain unchanged, but AI has made the evaluation of enforcement technologies more urgent.

Protect early, register globally and document ownership.

Keenan has interviewed legal and technology experts who've emphasized that creators should still register their IP under existing legal frameworks as early as possible and, when appropriate, across multiple jurisdictions.

Even though upfront costs can be high, delaying and failing to cast a wide net often proves more costly.

"Trademark squatting, design squatting happens all the time," Eriksson told Keenan. Bad actors monitor new brands and register first in other regions, forcing expensive legal fights.

"Trademark squatting, design squatting happens all the time,"

On the enforcement side, firms should consider adopting legal technology tools to protect IP. Detection tools can continuously scan marketplaces, social media and websites to identify infringing material. Image and video fingerprinting software can recognize altered or flipped copies. Some systems can even automate the first stages of the takedown strategy, including generating claims, compiling evidence and submitting notices.

Now is the time to build an AI-ready enforcement plan and stay current on the rapidly evolving case law and tools shaping IP protection. Sign up for a free CEB trial to explore its IP and technology resources for regularly updated analysis, case insights and practical tools designed for evolving case matters.

CEB

Contact us at 1-800-232-3444 or visit us online to learn more.