

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any **suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Cross-Border Intellectual Property Enforcement in the Global Digital Economy: Legal Frameworks, Jurisprudential Evolution and Contemporary Challenges

ROHAN GHOTI*, SWAMINI RAUT**, AND ADITI GUPTA***

ABSTRACT

The enforcement of intellectual property rights across national borders is one of the most structurally significant legal challenges of the digital age. The territorial foundations of intellectual property law, premised on physical infringement, identifiable defendants and localised harm, are wholly incompatible with a framework in which a single infringing act may originate in one country, pass through servers in a second, be monetised through payment processors in a third and reach consumers across fifty more within seconds. This paper examines the normative framework governing cross-border intellectual property enforcement, reviews the landmark judicial decisions that have shaped its development and analyses three frontier challenges, namely generative artificial intelligence, blockchain technologies and NFT markets, and platform liability divergence, that are altering the enforcement landscape in ways existing legal systems cannot accommodate. While negotiation and bilateral treaty-making remain natural instruments for resolving disputes, international courts and tribunals, together with specialist arbitral bodies and enforcement mechanisms, have become the most authoritative means of addressing complex and politically sensitive cross-border intellectual property disputes. This paper assesses the doctrinal significance of these developments in consolidating coherent enforcement methods, situates them within the global legal order, and addresses the destabilising effect of generative artificial intelligence on rights frameworks, the disruptive impact of blockchain technologies and decentralised digital asset markets, and the structural weaknesses of global adjudicatory discipline amid intensifying geopolitical competition. It concludes by outlining a set of policy-oriented reforms intended to improve the legitimacy, effectiveness and adaptability of the global enforcement framework.

Keywords: *Intellectual property, cross-border enforcement, digital economy, platform liability, TRIPS Agreement, blockchain technology, NFTs, generative artificial intelligence, jurisdictional harmonisation, notice-and-takedown.*

* Author is a student at D.E.S. Navalmal Firodia Law College (Fergusson), Pune, India.

** Author is a student at D.E.S. Navalmal Firodia Law College (Fergusson), Pune, India.

*** Author is a student at D.E.S. Navalmal Firodia Law College (Fergusson), Pune, India.

I. INTRODUCTION

Intellectual property law was built upon an explicitly territorial basis: rights are granted by sovereign states, enforced by national courts, and effective only within the jurisdiction that creates them. For most of the history of intellectual property law this arrangement functioned adequately. Physical counterfeiting required manufacturing infrastructure, warehousing and distribution networks, all of which left traceable evidence in identifiable jurisdictions. A rights holder could determine which country's law had been violated and pursue domestic remedies through familiar legal channels.

The digital economy has dismantled this correspondence entirely. Contemporary infringing enterprises are structured with deliberate complexity: servers hosted in one jurisdiction, commercial registration in another, payment processing in a third and consumers distributed globally. Blockchain-based NFT markets operate through decentralised infrastructure in which the operators are not situated in any single jurisdiction. Artificial intelligence systems now process copyrighted material on a global scale and generate relevant outputs across every legal system at once. The enforcement tools available to rights holders, including notice-and-takedown, site blocking and domain seizure, all operate within national boundaries that the most sophisticated infringers have learned to exploit with precision.

This paper addresses that structural gap directly. The jurisprudential developments identified below represent genuine and important doctrinal progress. The argument advanced here is that incremental adaptation of existing mechanisms is no longer sufficient, and that the structural shortcomings of the cross-border intellectual property enforcement system impose real and growing costs on creators, innovators and the broader public interest in a functioning digital economy. The stakes extend beyond the interests of large rights holders; they reach individual creators, small enterprises and the integrity of the informational commons on which digital innovation depends.

II. THE NORMATIVE FRAMEWORK: ARCHITECTURE AND STRUCTURAL DEFICIENCIES

A. The territorial principle

The territorial principle is the bedrock of international intellectual property law. Intellectual property rights are enforceable only within the jurisdiction that creates them and only by the courts and authorities of that jurisdiction. The *Paris Convention for the Protection of Industrial*

Property (1883) enshrined the independence of national patents and trademarks.¹ The *Berne Convention for the Protection of Literary and Artistic Works* (1886, as revised) confirmed that copyright protection is determined by the domestic law of each country.² This territorial structure was reinforced by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, 1994), which set out substantive minimum standards binding upon all 164 World Trade Organization (WTO) member states.³

The consequence of this architecture is structural and severe: a rights holder seeking to enforce intellectual property globally must engage the legal system of every jurisdiction in which infringement occurs. This reality systematically favours large, well-resourced rights holders able to sustain multi-jurisdictional litigation and systematically disadvantages individual creators and smaller enterprises for whom such engagement is economically prohibitive.

B. TRIPS: minimum standards and maximum variation

The TRIPS Agreement is the most ambitious multilateral intellectual property harmonisation effort to date. Its Part III enforcement provisions, requiring member states to provide accessible civil procedures, provisional measures, border enforcement measures and criminal penalties for wilful commercial-scale infringement, marked a real advance over previous treaties. For the first time, the binding dispute settlement mechanism of the WTO provided a means of state-to-state accountability for intellectual property enforcement failures.

Three structural deficiencies have become salient in the digital context. First, minimum standards invariably produce maximum variation: implementation discretion across 164 WTO members leads to dramatic differences in practice. Second, TRIPS was negotiated between 1986 and 1994, before the advent of the commercial internet, and does not address online infringement, the liability of internet service providers (ISPs), notice-and-takedown arrangements or digital rights management. Third, the state-to-state dispute settlement process is simply too slow to address the volume and velocity of digital infringement. Attempts to modernise the framework through the Anti-Counterfeiting Trade Agreement (ACTA) (2006-2011) were rejected by the European Parliament in July 2012.

¹ PARIS CONVENTION FOR THE PROTECTION OF INDUSTRIAL PROPERTY, Mar. 20, 1883, as revised at Stockholm, July 14, 1967, 828 U.N.T.S. 305.

² BERNE CONVENTION FOR THE PROTECTION OF LITERARY AND ARTISTIC WORKS, Sept. 9, 1886, as last revised at Paris, July 24, 1971, 1161 U.N.T.S. 30.

³ AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 (entered into force Jan. 1, 1995).

C. The WIPO internet treaties

The *WIPO Copyright Treaty* (WCT) and the *WIPO Performances and Phonograms Treaty* (WPPT), both concluded in December 1996, were the first international treaties to address the problem of digital distribution.^{4,5} The WCT recognised a right of communication to the public through on-demand digital delivery and required signatory states to protect technological protection measures and rights management information. The United States implemented the WCT in 1998 through the Digital Millennium Copyright Act, and the European Union did so through the Information Society Directive (2001/29/EC).⁶ Implementation has nonetheless been uneven and, most significantly, neither treaty provides any mechanism for cross-border enforcement cooperation between states.

D. Bilateral and regional instruments

Major intellectual property exporters have pursued TRIPS-plus standards through bilateral free trade agreements, including the United States-Mexico-Canada Agreement (USMCA, 2020), the European Union-Japan Economic Partnership Agreement, the European Union-South Korea Free Trade Agreement and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which provide for stronger copyright terms, ISP liability frameworks and anti-circumvention obligations.⁷ These instruments exhibit three principal weaknesses: they bind only their parties; they create a patchwork of obligations and lack an overarching enforcement architecture; and they are subject to political conditions that may change rapidly, as illustrated by the withdrawal of the United States from the Trans-Pacific Partnership in 2017.

III. ENFORCEMENT MECHANISMS: TOOLS, REACH AND LIMITS

A. Notice-and-takedown

Notice-and-takedown regimes, exemplified by Section 512 of the DMCA in the United States and Article 17 of the Copyright in the Digital Single Market Directive (2019/790/EU) in the European Union, condition platform safe-harbour protection on the rapid removal of infringing content.⁸ The mechanism offers practical advantages of low cost, speed and scalability. Its cross-border limitation is fundamental: it applies only to platforms subject to the law of the

⁴ WIPO COPYRIGHT TREATY, Dec. 20, 1996, 2186 U.N.T.S. 121 (entered into force Mar. 6, 2002).

⁵ WIPO PERFORMANCES AND PHONOGRAMS TREATY, Dec. 20, 1996, 2186 U.N.T.S. 203 (entered into force May 20, 2002).

⁶ Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998); Directive 2001/29/EC of the European Parliament and of the Council on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10.

⁷ United States-Mexico-Canada Agreement, ch. 20, entered into force July 1, 2020.

⁸ Digital Millennium Copyright Act § 512, 17 U.S.C. § 512; Directive 2019/790/EU of the European Parliament and of the Council on Copyright and Related Rights in the Digital Single Market, art. 17, 2019 O.J. (L 130) 92.

jurisdiction whose framework creates the obligation. Against platforms deliberately incorporated in non-cooperating jurisdictions, it provides no effective remedy.

B. Site blocking and ISP injunctions

Court orders compelling ISPs to block subscriber access to identified infringing websites address a gap that notice-and-takedown cannot fill: they reach foreign-operated platforms that have no domestic legal presence. Dynamic blocking regimes, under which injunctions may be extended in a timely manner to mirror sites and new IP addresses, have partly addressed site migration. Courts in the United Kingdom, Australia, Germany, France and Italy have consistently held that the limitations of blocking, including its geographical scope, the technical capacity for circumvention through VPNs and the maintenance burden, do not render it disproportionate to the objective of protecting rights holders from large-scale commercial infringement.

C. Financial and advertising pressure

Pressure on payment processors and advertising networks to terminate relationships with identified infringing sites lies outside formal legal process but has proved practically effective against commercial piracy operations dependent on subscription revenue and advertising income. Its diminishing effectiveness against operations using cryptocurrency payment systems or fully decentralised infrastructure is a growing concern, one that is compounded as blockchain-based infringement becomes more prevalent.

IV. JUDICIAL EVOLUTION: LANDMARK DECISIONS AND DOCTRINAL CONTRIBUTIONS

A. United States v. Megaupload Limited

The *Megaupload* prosecution remains one of the most instructive case studies in the limits of extraterritorial criminal intellectual property enforcement.⁹ At its height, Megaupload was the thirteenth most visited website worldwide, with some 50 million registered users and storing approximately 25 petabytes of data; its revenues were estimated at \$175 million, while rights holders were alleged to have lost approximately \$500 million.

On 19 January 2012, the United States Department of Justice unsealed a federal indictment against the company and seven individuals, including the founder Kim Dotcom, a German-Finnish citizen resident in New Zealand. The FBI simultaneously seized Megaupload's domain

⁹ *United States v. Megaupload Ltd.*, No. 1:12-cr-00003 (E.D. Va. indictment filed Jan. 5, 2012).

names, shutting down the global network in a coordinated operation across the United States, New Zealand and Hong Kong.

The case exposed three fundamental weaknesses. As to jurisdiction, the United States asserted criminal authority over a Hong Kong-incorporated company whose employees were largely European nationals resident in New Zealand, principally because seized servers were located in Virginia and the domain names were United States-registered, an expansive jurisdictional claim. In the New Zealand extradition proceedings, the High Court found that the online communication of copyrighted works was not a criminal offence under section 131 of the New Zealand Copyright Act 1994. In 2023, Ortmann and Van der Kolk were convicted in New Zealand. Kim Dotcom continued to resist extradition more than twelve years after his arrest, and the copyright allegations remain untested at trial. *Megaupload* demonstrates at once what maximal multilateral coordination can achieve and what it cannot.

B. L'Oreal v. eBay and Tiffany v. eBay

Taken together, these contemporaneous decisions on materially similar facts provide the clearest demonstration of the transatlantic enforcement gap at the centre of the cross-border platform liability problem. *L'Oreal* brought trademark infringement proceedings against eBay simultaneously in France, Belgium, England and Spain.¹⁰ The Court of Justice of the European Union (CJEU) established a passive/active distinction: where a platform takes an active role, for instance by optimising the presentation of listings or promoting offers, it cannot claim that its hosting is shielded from liability under Article 14 of the E-Commerce Directive (2000/31/EC). Equally, awareness that listings may be infringing, coupled with a failure to act, removes the protection.

In *Tiffany v. eBay*, the Second Circuit took a different view of materially similar facts.¹¹ United States law requires specific knowledge of particular infringing listings together with a failure to act, and general knowledge that counterfeits are circulating on a platform is insufficient. eBay was held to have discharged its notice-and-takedown obligations. The same platform, with the same operational knowledge, is therefore subject to liability that differs according to which side of the Atlantic the court sits on. The subsequent enactment of Article 17 of the Digital Single Market Directive, which requires proactive upload filtering, has widened this transatlantic divergence still further.

¹⁰ *L'Oreal SA v. eBay Int'l AG*, Case C-324/09, [2011] E.C.R. I-6011 (CJEU).

¹¹ *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).

C. Cartier International v. British Sky Broadcasting

The *Cartier* litigation is the leading authority on ISP site-blocking injunctions in the common law world.¹² Cartier International sought injunctions requiring five major United Kingdom ISPs to block access to websites selling counterfeit luxury goods, operated entirely from abroad by unknown persons with no domestic presence. Arnold J granted the orders, which were the first United Kingdom website-blocking injunctions to protect trademark rather than copyright, in reliance on Article 11 of the EU Enforcement Directive (2004/48/EC).

The Court of Appeal established the governing proportionality framework: blocking must be necessary, effective to a meaningful degree, dissuasive, proportionate in its interference with third-party interests, and fair to affected parties. The Supreme Court upheld the injunctions in 2018 but required rights holders, rather than ISPs, to bear the costs of implementation and ongoing maintenance. The *Cartier* proportionality framework has been expressly adopted by Australian courts in *Roadshow Films Pty Ltd v. Telstra Corporation Ltd*¹³ and applied consistently across European Union member states.

D. Hermes International v. Ledger SAS (MetaBirkins)

The *MetaBirkins* case is the first major decision at the intersection of trademark law, blockchain infrastructure and NFT market development.¹⁴ Mason Rothschild minted and sold 100 NFTs depicting fur-covered versions of the iconic Birkin handbag of Hermes on the Ethereum blockchain through OpenSea, generating roughly \$1.1 million in sales. Hermes brought claims for trademark infringement and dilution in the Southern District of New York.

The central legal question was whether the NFTs constituted protected artistic expression under the First Amendment, applying the test in *Rogers v. Grimaldi*,¹⁵ and, if so, whether they nonetheless amounted to actionable infringement. In February 2023, the jury found for Hermes and awarded \$133,000 in damages, on the basis that the Birkin mark was clearly misleading as to source or sponsorship. *MetaBirkins* establishes that United States trademark rights extend to NFTs. Germany, Japan, South Korea and most other jurisdictions have yet to address the relationship between domestic trademark law and blockchain-created digital assets, and considerable uncertainty as to their global legal status remains to be resolved.

¹² *Cartier Int'l AG v. British Sky Broad. Ltd.*, [2014] EWHC (Ch) 3354; [2016] EWCA (Civ) 658; [2018] UKSC 28.

¹³ *Roadshow Films Pty Ltd v. Telstra Corp. Ltd.* [2016] FCA 1503 (Austl.).

¹⁴ *Hermes Int'l v. Rothschild*, No. 22-cv-00384 (S.D.N.Y. jury verdict Feb. 8, 2023).

¹⁵ *Rogers v. Grimaldi*, 875 F.2d 994 (2d Cir. 1989).

E. The New York Times v. Microsoft and OpenAI

Filed on 27 December 2023, this is the most significant ongoing litigation in global intellectual property enforcement in the age of artificial intelligence.¹⁶ Both defendants are alleged to have trained large language models on millions of *New York Times* articles without authorisation, and to have produced systems that reproduce verbatim passages of Times journalism in response to ordinary user prompts, including content otherwise accessible only through a paid subscription.

The case turns on the fair use doctrine (17 U.S.C. § 107). The artificial intelligence developers contend that model training is transformative, analogous to the full-text indexing approved in *Authors Guild v. Google Inc.*¹⁷ The Times argues that training is not transformative where it serves a clear commercial purpose, where the outputs compete with the originals, and where the capacity to reproduce protected expression verbatim creates market substitution. Articles 3 and 4 of EU Directive 2019/790 provide text and data mining exceptions that differ markedly from the United States fair use standard. Japanese guidance indicates that artificial intelligence training does not, as a general matter, constitute infringement. The United Kingdom is developing a post-Brexit framework that remains uncertain. Models trained in permissive jurisdictions are deployed worldwide, and whether such deployment will give rise to liability in a stricter regime remains an open question.

V. COMPARATIVE DOCTRINAL ANALYSIS

The landmark decisions examined above may be set out comparatively to illuminate their respective doctrinal contributions. *Megaupload* exposes the outer limits of extraterritorial criminal enforcement and the dependence of coordinated action on multilateral cooperation. The parallel decisions in *L'Oreal* and *Tiffany* crystallise the transatlantic divergence in platform liability, turning on the contrast between the active-role analysis of the CJEU and the specific-knowledge requirement of United States law. *Cartier* establishes and refines the proportionality framework for ISP site-blocking injunctions in the common law world. *MetaBirkins* marks the frontier of NFT trademark enforcement, confirming that established trademark doctrine extends to blockchain-created assets while leaving global characterisation unresolved. The *New York Times* litigation presents, for the first time at scale, the question whether the training of generative artificial intelligence on copyrighted works falls within the fair use doctrine.

¹⁶ *N.Y. Times Co. v. Microsoft Corp.*, No. 23-cv-11195 (S.D.N.Y. filed Dec. 27, 2023).

¹⁷ *Authors Guild v. Google Inc.*, 804 F.3d 202 (2d Cir. 2015).

Case	Forum & Year	Key Doctrinal Contribution	Lasting Significance
Megaupload	US/NZ, 2012–	Extraterritorial criminal enforcement; limits of criminal secondary liability for platform operators	Defined reach and structural limits of US authority against foreign digital infringers
L'Oreal v. eBay	CJEU, 2011	Passive/active platform distinction; proactive injunctions under EU law	Established EU platform liability framework; crystallized transatlantic divergence from US doctrine
Tiffany v. eBay	2d Cir., 2010	Specific knowledge standard; notice-and-takedown satisfies US legal obligations	US platform liability baseline; starkly contrasted with EU active/passive framework
Cartier v. BSKyB	UK, 2014–18	Proportionate ISP site-blocking across all IP rights; costs allocation framework	Extended blocking beyond copyright; adopted across common law world and EU
Hermes v. MetaBirkins	S.D.N.Y., 2023	Trademark rights extend to NFT contexts; Rogers test applied to digital assets	First US IP determination in blockchain/NFT markets; global uncertainty persists
Apple v. Samsung	Multi-juris., 2011–18	Contradictory outcomes across ten jurisdictions on identical infringement	Most compelling demonstration of TRIPS harmonization's practical failure
NYT v. Microsoft/OpenAI	S.D.N.Y., 2023–	Copyright infringement through AI training data; fair use in machine learning	Defining AI-era enforcement case; global impact of divergent national frameworks

Table: Comparative overview of the landmark cross-border intellectual property enforcement decisions.

VI. FRONTIER CHALLENGES

A. Generative artificial intelligence and training data

The artificial intelligence training data problem represents a qualitative shift, not merely an incremental extension of the cross-border enforcement problem. The training of large-scale artificial intelligence systems has involved the ingestion of copyrighted text, images, audio and video on an unprecedented scale: tens of billions of tokens scraped from the internet, including the published works of millions of creators, ingested without authorisation, compensation or notification. The value of the resulting models is directly affected by the quality and diversity of the training data, creating an economic incentive to consume material in a manner that existing law does not adequately address.

Divergence among national legal frameworks creates strong regulatory arbitrage incentives that influence where artificial intelligence companies locate their training operations, how those companies are organised, and ultimately how the commercial value of generative artificial intelligence is shared between technology developers and the creators whose work underpins it. Models trained in jurisdictions with permissive copyright laws are deployed globally and accessed in jurisdictions with restrictive copyright laws, yet the legal consequences of such

deployment are not clearly defined in every jurisdiction. The output dimension is more complex still: where artificial intelligence systems generate content closely reproducing copyrighted training material, infringement claims may arise in every jurisdiction in which those outputs are viewed.

B. Blockchain technology, NFTs and the decentralised enforcement problem

Blockchain technology presents the cross-border enforcement system with a structurally novel challenge that differs from all previous digital enforcement problems in both nature and degree. Earlier enforcement challenges, such as locating infringing content, identifying a responsible platform and applying national law, did not call the concept of territorial enforcement into question. Decentralised blockchain infrastructure removes or fundamentally contests all three elements at once.

C. Blockchain as a rights management tool

On-chain registration of copyright and trademark ownership carries genuine enforcement benefits. Blockchain timestamps furnish verifiable, cryptographically secured and tamper-resistant evidence of prior creation and ownership that has been accepted as probative in several domestic cases. Smart contract licensing, under which royalty obligations are embedded in the code governing NFT transfers so that rights holders are automatically paid upon every resale, is a theoretically powerful mechanism for automated cross-border rights management that operates independently of any particular country's legal system.

D. NFTs and the decentralised enforcement problem

The *MetaBirkins* decision concerns the most legally straightforward variant of the NFT enforcement problem: a named defendant, an identifiable intermediary platform, and a United States nexus sufficient to ground federal jurisdiction. The harder and more interesting cases involve NFTs created through genuinely decentralised protocols with no identifiable operator, sold through decentralised autonomous organisations (DAOs) that distribute legal responsibility among anonymous token holders, and stored on decentralised file systems such as IPFS across globally distributed nodes. In such cases there is no notice-and-takedown; no domain name can be blocked; and no payment processor can be compelled to act. The enforcement toolkit developed over three decades of digital intellectual property law is wholly inapposite to genuinely decentralised infrastructure.

Where a copyright-infringing NFT is minted on the Ethereum blockchain, a permissionless global network of nodes spread across dozens of countries, the question arises as to where the infringing act actually took place. Some United States courts have applied effects-test reasoning

to assert jurisdiction where NFT sales clearly targeted United States consumers. Effects-test reasoning, however, does not extend to genuinely anonymous and genuinely decentralised conduct.

E. Platform liability divergence and regulatory arbitrage

The deepening divergence between the United States Section 512 safe-harbour framework, the European Union Article 17 proactive filtering obligation and emerging regulatory frameworks across Asian jurisdictions produces increasing compliance complexity for platforms operating in multiple markets and a structural bias in favour of large incumbents with the resources to satisfy divergent regulatory requirements. China has moved towards a 'red flag' regime requiring proactive monitoring by platforms that have systemic knowledge of infringement. Japan and South Korea maintain distinct systems that continue to evolve under technological and commercial pressure. There is at present no multilateral instrument addressing this divergence, and no political support for such a mechanism.

VII. POLICY RECOMMENDATIONS AND INSTITUTIONAL REFORMS

A. Harmonise choice-of-law rules for digital IP infringement

The international community should move swiftly to develop agreed choice-of-law rules for digital intellectual property infringement and to establish the *lex loci protectionis* principle, under which the applicable law is that of the country for which protection is claimed, as the default rule through a binding instrument concluded under the auspices of WIPO or the Hague Conference on Private International Law. This reform is particularly important for blockchain-based infringement, where the absence of agreed rules is generating enforcement paralysis and enabling infringing actors to exploit the resulting indeterminacy with impunity.

B. A dedicated international framework for blockchain and digital assets

WIPO should convene a dedicated intergovernmental process, modelled on the 1996 internet treaties process that produced the WCT and WPPT, to establish internationally agreed principles on the characterisation of NFTs in relation to underlying intellectual property rights; jurisdictional rules for blockchain-based infringement; on-chain registration recognised as valid within domestic formal registration regimes; and minimum standards for the technical and legal enforcement of smart contract licensing obligations. In the absence of such an instrument, major blockchain platforms with identifiable operators should be required, as a condition of obtaining operating licences in major jurisdictions, to maintain intellectual property rights verification systems prior to the issuance of digital assets.

C. Converge platform liability standards

The divergence between the United States, the European Union and Asia in platform liability frameworks should be addressed through an international minimum standards instrument setting agreed criteria for safe-harbour qualification, agreed knowledge thresholds triggering platform liability, and agreed minimum proactive responsibilities for very large platforms with systemic knowledge of infringement. Absent meaningful convergence, regulatory arbitrage will persist as artificial intelligence and decentralised technologies devise new ways of structuring infringing operations to exploit divergent national standards. Such an instrument need not impose full uniformity; it should establish a floor against the most egregious instances of jurisdiction-shopping.

D. An international AI training data framework

The ongoing WIPO discussions on artificial intelligence and intellectual property policy should advance towards a binding or quasi-binding instrument developing agreed principles on: whether the training of artificial intelligence on copyrighted works requires prior authorisation and ongoing compensation; the scope, accessibility and retroactive applicability of opt-out mechanisms for rights holders; minimum transparency standards for artificial intelligence developers as to the provenance and licensing status of training datasets; and accountability frameworks where artificial intelligence systems produce outputs that substantially reproduce protected expression. At present, the fragmentation between the United States, the European Union, Japan and the United Kingdom creates precisely the regulatory arbitrage conditions the international intellectual property system was designed to prevent.

E. Establish a multilateral enforcement cooperation mechanism

A multilateral intellectual property enforcement cooperation mechanism, modelled on the frameworks for financial crime cooperation and cybercrime coordination established by the Budapest Convention, should be created to provide rapid, practical information sharing between national law enforcement agencies, coordinated cross-border takedowns of large-scale infringement operations, and joint investigation of commercial-scale piracy organisations that exploit jurisdictional fragmentation. Existing mutual legal assistance treaty frameworks must be reformed to reduce processing times for intellectual property-related requests, which currently run to years and are incompatible with the speed of digital infringement.

VIII. CRITICAL EVALUATION

The international adjudicatory and enforcement framework for cross-border intellectual property disputes has achieved considerably more than its critics sometimes acknowledge. A field that half a century ago was characterised by doctrinal instability, methodological inconsistency and recourse to unilateral assertion of rights has been transformed into one of recognised legal principles, accessible enforcement mechanisms and a measure of international accountability that did not previously exist.

At the same time, significant limitations must be confronted with intellectual honesty. The gap between the formal ambition of the TRIPS framework and the practical reality of enforcement against sophisticated digital infringers has widened, not narrowed, since 1994. The emergence of blockchain-based decentralised markets and globally trained artificial intelligence systems creates enforcement problems that existing tools were not designed to address and that cannot be resolved by incremental modification alone. The political will required to address these problems through the multilateral processes that effective reform demands has so far been absent.

The legitimacy of the international intellectual property system ultimately rests on its capacity to provide meaningful protection to rights holders of all sizes, in all jurisdictions and across all technological contexts, and that capacity is now severely depleted. The recommendations advanced in this paper are not a blueprint for perfection but a minimum programme of adaptation necessary to preserve the functional integrity of a system from which both rights holders and the public benefit significantly.

IX. CONCLUSION

Cross-border intellectual property enforcement in the global digital economy is marked by a structural gap that the international community has not yet honestly or comprehensively confronted. The tools available to rights holders, including notice-and-takedown, site blocking, domain seizure and financial pressure on intermediaries, were built for a world of centralised platforms, identifiable defendants and geographically determined infringing acts. That world is fading. Blockchain-based decentralised markets, generative artificial intelligence systems trained in permissive jurisdictions and deployed globally, and deepening platform liability divergence are generating enforcement challenges that existing mechanisms cannot address.

The jurisprudential developments examined in this paper, from the limits of extraterritorial criminal enforcement exposed by the *Megaupload* prosecution, through the transatlantic platform liability divergence crystallised by the parallel *L'Oreal* and *Tiffany* decisions, the ISP

blocking framework established and refined in the *Cartier* litigation, the NFT trademark frontier marked by the *MetaBirkins* verdict, and the artificial intelligence training data question presented in the *New York Times* litigation, represent genuine doctrinal progress: courts applying established legal frameworks thoughtfully to facts their designers never anticipated.

What courts cannot do, and should not be expected to do, is generate the multilateral political commitment that effective cross-border enforcement ultimately requires. Harmonised choice-of-law rules, converged platform liability standards, dedicated international frameworks for blockchain and artificial intelligence, and operational enforcement cooperation between national authorities all require states to subordinate short-term regulatory preferences to the shared recognition that a global digital economy without genuine intellectual property enforcement is unsustainable. Securing that recognition is the central challenge for the next generation of international intellectual property governance, and its costs, if it is not secured, will ultimately fall on the creators, innovators and citizens whose work and welfare the system nominally exists to serve.

X. BIBLIOGRAPHY

1. Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015).
2. Margaret Chon, *NFTs and Intellectual Property*, 95 TEMP. L. REV. 423 (2023).
3. Graeme B. Dinwoodie, *A New Copyright Order: Why National Courts Should Create Global Norms*, 149 U. PA. L. REV. 469 (2000).
4. Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567 (2012).
5. Peter K. Yu, *The International Enclosure Movement*, 82 IND. L.J. 827 (2006).
6. Pamela Samuelson, *Evolving Conceptions of Copyright Subject Matter*, 78 U. PITT. L. REV. 17 (2016).
7. Primavera De Filippi & Aaron Wright, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, HARV. J.L. & TECH. (2018).
8. Eliza Mik, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 9 LAW, INNOVATION & TECH. 269 (2017).
9. MIHALY FICSOR, *THE LAW OF COPYRIGHT AND THE INTERNET: THE 1996 WIPO TREATIES, THEIR INTERPRETATION AND IMPLEMENTATION* (2002).

10. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).
11. SAM RICKETSON & JANE C. GINSBURG, INTERNATIONAL COPYRIGHT AND NEIGHBOURING RIGHTS: THE BERNE CONVENTION AND BEYOND (2d ed. 2006).
12. PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018).
13. GRAEME B. DINWOODIE & ROCHELLE C. DREYFUSS, A NEOFEDERALIST VISION OF TRIPS: THE RESILIENCE OF THE INTERNATIONAL INTELLECTUAL PROPERTY REGIME (2012).
14. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008).
15. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).
16. *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).
17. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).
18. *Viacom Int'l Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).
19. *Samsung Elecs. Co. v. Apple Inc.*, 580 U.S. 53 (2016).
20. *Unwired Planet Int'l Ltd v. Huawei Techs. Co. Ltd* [2020] UKSC 37.
