FROM BIRKIN TO METABIRKIN: TRADEMARK PROTECTION AND ENFORCEMENT IN THE AGE OF NFTS

Zoha Khanam, LL.M. (Intellectual Property Law and Management)
National Law University Delhi.

ABSTRACT

The metaverse is no longer a distant fantasy. It is a rapidly growing digital world where people buy, sell, and create every day. But as this virtual universe expands, our laws are struggling to keep up. This paper explores one of the most urgent legal paradoxes of our time: the metaverse is completely borderless, yet our intellectual property laws are strictly territorial.

Through an examination of landmark cases like Hermès v. Rothschild, evolving trademark classification systems, and cross-border enforcement frameworks, this paper reveals how traditional legal tools simply were not built for a decentralised digital world. From anonymous avatars hiding behind blockchain wallets to infringing NFTs that cannot be deleted, the challenges are both complex and immediate. This paper further analyses how courts in the United States and European Union are attempting to balance trademark protection with freedom of expression, and how jurisdictions are racing to localise infringements that happen everywhere and nowhere at once. On the jurisdictional front, the paper evaluates three competing approaches to localize online infringements and contrasting the US's flexibility against the codified formalism of EU's frameworks. It also addresses other enforcement challenges unique to decentralized environment and emphasizes on AI-driven monitoring, dynamic+ injunction, and international legal harmonization as pathways for metaverse to thrive as a safe and innovative digital frontier.

INTRODUCTION

The internet has grown and changed dramatically over the last few decades. In its early days, we experienced Web 1.0. This was often called the static web. It functioned like a digital library where users were simply passive consumers of information. Then, the internet evolved into Web 2.0. This era brought us social media and highly interactive websites. People went from just reading text to actively creating content, sharing ideas, and building online communities. Today, we are stepping into the next major phase of digital evolution, known as Web 3.0 and the metaverse. The metaverse is a deeply immersive, three-dimensional digital universe. It uses technologies like virtual reality, augmented reality, and blockchain to build decentralized environments. In these new virtual spaces, users can control digital avatars, buy virtual items, and socialize in a world that feels incredibly real.

However, this amazing technological leap brings a massive legal problem. Legal experts often refer to this issue as a core paradox. The metaverse is designed to be a completely global and borderless space. Users from completely different countries can easily meet, trade digital assets, and explore together without facing any physical boundaries. In sharp contrast, our intellectual property rights are strictly territorial.[1] This means that the law only protects a trademark or a copyright within the specific physical borders of the country that granted the protection. This creates a fundamental clash. We now have a truly borderless virtual ecosystem operating under a legal framework that relies entirely on physical borders and national sovereignty. For instance, a user in Japan could buy a digital item from a creator in France on a platform hosted by a global network. If that digital item copies a famous brand, it is very hard to decide which country's laws should apply.

This clash means that the transition to Web 3.0 completely disrupts traditional intellectual property frameworks. Our current laws were built for a physical world with clear borders and tangible products. They were not designed for a decentralized digital space where virtual goods move instantly across the globe. Because the old rules no longer fit perfectly, the legal system faces a serious crisis. Therefore, we must deeply reevaluate how we manage intellectual property in this new era. We need new strategies to figure out exactly how we localize an infringement when it happens in a virtual space. We also need to figure out how to establish

[1] World Intellectual Property Organization, *The Localization of IP Infringements in the Online Environment: From Web 2.0 to Web 3.0 and the Metaverse – Executive Summary*, WIPO/ACE/16/10/EX ¶ 12 (Oct. 26, 2023), https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_16/wipo_ace_16_10-executive_summary1.pdf.

proper court jurisdiction when the users are anonymous or scattered around the world. Finally, we must discover new ways to effectively enforce trademark and copyright protections so that creators and brands remain safe in the metaverse.

THE METAVERSE ECOSYSTEM AND DIGITAL ASSETS

Metaverse: Unpacking the New Reality.

To understand the metaverse, we must first look at the technology that builds it. The metaverse can be understood as an interconnected system of digital environments in which users engage with one another simultaneously and continuously. It relies on several core technologies to create a deeply immersive experience. *Virtual reality*, or *VR*, uses special headsets to completely surround the user in a computer-generated digital world. It replaces what you see and hear with a new digital environment.[2] *Augmented reality*, or *AR*, takes a different approach. It uses glasses or screens to place digital images over the physical world we see around us.[3] Together, these tools allow users to step inside the internet instead of just looking at a flat screen. Behind the visual scenes, the metaverse relies heavily on blockchain technology. Blockchain functions as a tamper-resistant, distributed record-keeping system that logs all transactions permanently across a wide network of computers simultaneously. This technology makes it possible to create and trade *Non-fungible tokens*, commonly known as NFTs. NFTs act as unique digital certificates stored on the blockchain. They prove that a person truly owns a specific digital asset. This could be a piece of digital art, a video clip, or a virtual item.[4] Because NFTs cannot be copied or replaced, they create real scarcity and value in the digital world.[5]

There is no single, connected metaverse right now. Instead, the digital landscape consists of many different virtual platforms.[6] Today's virtual platforms can broadly be divided along a spectrum defined by who holds governance authority, those controlled by a single company and those managed collectively by their communities: *centralized* and *decentralized*.

---

[2] Carlos Cantú, Cecilia Franco & Jon Frost, *The Economic Implications of Services in the Metaverse*, BIS Papers No. 144, at 3 (Bank for Int'l Settlements, Monetary & Economic Dep't, Feb. 2024).
[3] *Id.* at 28.
[4] Alexandra Chiroșca, *Navigating the Metaverse: Legal Challenges and Trademark Protection*, 1 Intellectus 48, 49 (2024).
[5] *Yuga Labs, Inc. v. Ripps*, No. 24-879, slip op. at 7 (9th Cir. July 23, 2025).
[6] International Trademark Association, *Trademarks in the Metaverse*, at 13 (Apr. 2023), https://www.inta.org/wp-content/uploads/public-files/perspectives/industry-research/METAVERSE_REPORT-070323.pdf.

A ***centralized metaverse*** is owned and controlled by a single corporate entity. This company builds the world, makes all the final decisions, enforces the rules, and controls the digital payment systems. Users must follow the platform's specific terms of service. Popular examples of centralized platforms include Meta's Horizon Worlds and the massive gaming platform Roblox.

In contrast, a ***decentralized metaverse*** operates on Web 3.0 principles and blockchain networks. Instead of one company holding all the power, these platforms are largely governed by their own users. They achieve this by using a structure called a Decentralized Autonomous Organization, or DAO.[7] In a DAO, users who hold specific digital tokens can vote directly on platform rules, content moderation, and future developments. Decentraland and The Sandbox are two major examples of decentralized metaverses. In these open spaces, users have true ownership of their digital items. They can also trade their virtual assets on outside cryptocurrency exchanges.

Click, Own, Exist: The Rise of Virtual Commerce

This new digital frontier has sparked a massive boom in virtual commerce. People and businesses are spending real money to buy digital items. The virtual economy is growing rapidly and holds immense economic value. In decentralized worlds like Decentraland and The Sandbox, users can actually purchase parcels of virtual real estate. These digital plots of land are bought and sold as NFTs. The value of this virtual land often mimics real estate prices in the physical world. Sometimes, prime virtual locations sell for hundreds of thousands of dollars. Beyond real estate, the market for virtual fashion and avatar accessories is also exploding. Users want their digital avatars to look unique and stylish. Because of this demand, major fashion brands are creating and selling digital clothing, sneakers, and accessories. For instance, famous luxury brands like Gucci and Balenciaga have opened virtual stores to sell digital fashion items. Some virtual dresses and digital sneakers have sold for thousands of dollars.[8] People also buy digital luxury handbags and rare digital art pieces. Businesses are quickly realizing that selling virtual products can be incredibly profitable and overall economic

[7] WIPO, *supra note* 1, ¶ 5, at 2.

[8] Crowell & Moring LLP, Retail in the Metaverse and Beyond, at 3 (Mar. 6, 2023), https://www.crowell.com/a/web/sWkmSmLUYTnE5j9oKRe8M3/retail-in-the-metaverse-and-beyond.pdf. *("Property in the metaverse is no new frontier to experienced users. Second Life, largely considered one of the first true 'metaverses' in a 3D format, began selling virtual land in 2003. Today's pricing for a 65,000-square-meter parcel on a premier island on Second Life costs $349 dollars, with a $229 monthly maintenance fee.").*

stakes being very high in Metaverse.[9] They do not have to pay for raw materials or physical factories. As the metaverse grows, this thriving digital marketplace will only continue to expand. It will fundamentally reshape how we think about ownership, retail, and global trade.

SUBSTANTIVE TRADEMARK CHALLENGES IN VIRTUAL WORLD

Static Classes in the Dynamic markets

As businesses enter virtual worlds, they face new legal hurdles regarding trademarks. A major challenge involves trademark registration and the *Nice Classification system*.[10] This international system categorizes goods and services into forty-five distinct classes for trademark registration. In the physical world, classification is mostly straightforward. A physical shoe falls into *Class 25* for clothing and footwear. However, a virtual shoe cannot be worn in real life, so it does not fit neatly into this physical category. Instead, a virtual item is essentially a piece of software or digital code. Because of this, trademark offices generally require virtual goods to be registered in classes related to technology and digital services. There is a strong current trend of brands filing new trademark applications to cover these digital spaces. Companies typically seek protection under the *Class 9* covering technology-based downloadable goods, particularly those whose ownership is verified through non-fungible tokens. They also file under *Class 35* for virtual retail store services, which cover online marketplaces for virtual goods. Additionally, brands use *Class 41* to protect virtual entertainment services, such as hosting virtual concerts or fashion shows. Finally, *Class 42* is used for technological services, including the design of virtual worlds or providing non-downloadable virtual goods.[11] This shift forces companies to expand their trademark portfolios to ensure they are fully protected in the digital realm.

Trademark Use and Brand Expansion into Virtual Markets

Beyond registration, the transition to the metaverse complicates the legal concept of trademark use. In traditional trademark law, protecting a mark often requires showing that it is actively

[9] Sakina Anwer & Tariq Hussain, *Intellectual Property Rights in the Metaverse: Legal Framework and Future Prospects*, 2 Contemp. J. Soc. Sci. Rev. 6, 7 (2024).
[10] Established under Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks, June 15, 1957, 550 U.N.T.S. 45.
[11] David Tan, *Trade Marks in the Metaverse*, Ctr. for Tech., Robotics, Artificial Intelligence & the L. (May 2024), https://law.nus.edu.sg/trail/trademarks-in-the-metaverse/ (see section III, *"The Use of Trademarks in the Metaverse"*).

used in commerce. This means the mark must be attached to goods or services that are sold or advertised to the public. In virtual worlds, this applies when selling digital items, such as avatar accessories or virtual real estate. A significant debate right now is whether virtual goods fall into the '***natural zone of expansion'*** for physical brands.[12] The *natural zone of expansion* is a legal doctrine. It allows a trademark owner to claim rights over a new product category if consumers would naturally expect the brand to expand into that area. For example, if a brand sells physical dresses, a consumer might reasonably expect them to sell physical scarves. However, legal experts and brand owners have no certainty that a court will view a virtual good as a natural expansion of a physical good. It is highly debated whether a digital image of a handbag is a natural extension of making actual leather handbags. Because of this uncertainty, brands cannot safely rely only on their physical trademark registrations to protect them in the metaverse.[13] They must actively use their marks in digital commerce and file new applications to ensure full protection.

Trademark Harm: Infringement and Dilution

When unauthorized users apply famous trademarks to digital assets, it often leads to trademark infringement. The core test for trademark infringement is whether the unauthorized use causes a likelihood of consumer confusion. Courts look at several factors to decide if consumers will be confused. They consider the strength of the original trademark, how similar the two marks are, and whether the person using the mark acted in bad faith. In the metaverse, an unauthorized creator might design a digital outfit featuring a well-known fashion logo. If a consumer buys this digital outfit thinking it was made or officially sponsored by the original brand, consumer confusion has occurred. This confusion harms the original brand because the consumer associates the brand with a digital product it did not actually create, control, or approve.

Even if there is no direct consumer confusion, unauthorized digital assets can still harm a brand through trademark dilution. Dilution doctrine shields marks from exploitations that erode their distinctiveness or cast a negative light on the brand's standing in the public eye.. This typically happens in two ways:

[12] Lorraine Tay & Audrey Lim, *Of Luxury Bags and Soup Cans — What if the MetaBirkins Case Was Fought in Singapore?*, Bird & Bird (Mar. 6, 2023), https://www.twobirds.com/en/insights/2023/singapore/of-luxury-bags-and-soup-cans-what-if-the-metabirkins-case-was-fought-in-singapore.
[13] Int'l Trademark Ass'n, supra note 6, at 10.

The first is ***dilution by blurring***. Blurring occurs when a famous mark is repeatedly used on unrelated products.[14] Over time, the mark loses its distinctiveness and its strong, singular association with the original brand.[15] In a virtual world, if a famous physical brand name is constantly used on random digital items, its unique selling power slowly fades.

The second form of ***dilution is tarnishment***. Tarnishment happens when an established mark becomes associated with substandard or objectionable material, thereby degrading the prestige and positive image that the brand has carefully cultivated. This damages the positive reputation of the famous mark. If a luxury brand's logo is used on poorly designed virtual items or in a virtual space with inappropriate content, it severely tarnishes the brand's prestigious image.[16]

The landmark legal case of ***Hermès International versus Mason Rothschild***[17] perfectly illustrates these substantive trademark challenges. In late 2021, a digital artist named Mason Rothschild created a collection of one hundred non-fungible tokens. He called this collection MetaBirkins. Each digital token was linked to an image of a blurry, faux-fur covered handbag that looked almost exactly like the famous Birkin bag made by the luxury fashion house Hermès. Rothschild sold these digital tokens online, and the collection quickly became very successful, generating over one million dollars in sales.[18] Hermès did not authorize this project and quickly filed a lawsuit against Rothschild. The fashion house accused the artist of trademark infringement, trademark dilution, and cybersquatting.

The dispute highlighted the deep-seated conflict that exists between the rights of trademark owners to protect their marks and the freedom of artistic expression. Hermès argued that the MetaBirkins project confused consumers and diluted the exclusive value of the real Birkin brand. Hermès presented evidence that magazines and people on social media actually believed Hermès was involved in the digital project.[19] In his defense, Rothschild claimed that he was

[14] Thayssa Bohadana Martins, *Beyond the Bag: MetaBirkins, Hermès, and the Legal Frontier of NFTs in Trademark Law*, 10 U. Bologna L. Rev. 136 (2025).
[15] Ariane Takano, *Diluted Reality: The Intersection of Augmented Reality and Trademark Dilution*, 17 Chi.-Kent J. Intell. Prop. 198 (2018).
[16] *Id.* at 199.
[17] For the facts of the case, see *Hermès Int'l v. Rothschild,* No. 22-cv-384 (JSR), slip op. at 3–4 (S.D.N.Y. Feb. 2, 2023).
[18] Zachary Small, *Hermès Wins MetaBirkins Lawsuit; Jurors Not Convinced NFTs Are Art*, N.Y. Times (Feb. 8, 2023), https://www.nytimes.com/2023/02/08/arts/hermes-metabirkins-lawsuit-verdict.html ("*Rothschild has estimated that he made about $125,000 from the NFTs, including the initial sales and royalties*.").
[19] *HERMES INTERNATIONAL and HERMES OF PARIS, INC. v. "MASON ROTHSCHILD"* a/k/a SONNY ESTIVAL, 1:22-cv-00384, (S.D.N.Y. Oct 07, 2022) ECF No. 67. (See at 15, ¶ 21)

not selling commercial products. Instead, he argued that his digital bags were art. Rothschild maintained that the collection was conceived as a critical artistic statement addressing the luxury fashion sector's longstanding reliance on exotic animal materials, specifically focusing on Hermès's use of exotic animal leather. Because it was art, Rothschild argued his work was protected by the First Amendment right to free speech.[20] To decide this, the court used a specific legal test called the Rogers test. This test asks if the use of the trademark has artistic relevance and if it explicitly misleads the public. Ultimately, a federal jury decided in favor of Hermès. The jury found that Rothschild was liable for trademark infringement and dilution. They concluded that his digital tokens functioned as commercial products rather than protected artistic commentary. They also found that he intentionally designed the digital bags to mislead consumers into believing that Hermès endorsed the project.[21] This pivotal decision confirmed that traditional trademark rights in the physical world can indeed be enforced against unauthorized digital assets in the metaverse.

BALANCING IP PROTECTION WITH FREEDOM OF EXPRESSION

As the digital landscape evolves, a profound legal tension has emerged between the strict enforcement of intellectual property rights and the fundamental human right to free speech. Trademarks are inherently designed to protect consumers from confusion and safeguard the goodwill that a brand has built. However, trademarks are also cultural symbols. Artists, commentators, and everyday internet users frequently use these recognizable symbols to express ideas, criticize society, or simply make a joke. When a creator incorporates a famous brand into a virtual good, a video game, or a social media post, courts must carefully balance the trademark owner's right to protect their brand against the creator's right to freedom of expression. Different legal systems approach this delicate balancing act in distinct ways.

U.S.'s Rogers Test: From Films to NFTs

In the United States, courts have traditionally navigated the conflict between the Lanham Act, the primary federal trademark statute, and the First Amendment using a framework known as

[20] U.S. Const. amend. I. (The First Amendment to the United States Constitution guarantees freedom of speech and expression. In the trademark context, courts have recognised a narrow exception to trademark liability for expressive works under the Rogers test, which requires that the use of a mark have artistic relevance to the work and not be explicitly misleading as to its source.)

[21] Loeb & Loeb LLP, *Hermès International v. Rothschild* (June 23, 2023), https://www.loeb.com/en/insights/publications/2023/06/hermes-international-v-rothschild.

the Rogers test. This legal standard originated from the 1989 case of ***Rogers v. Grimaldi***[22], where the famous dancer Ginger Rogers sued the creators of a film titled "Ginger and Fred," which followed two fictional cabaret performers who imitated her famous routines. In deciding the case, the Second Circuit Court of Appeals established a *two-prong test* to protect creative expression. Under the Rogers test, the unauthorized use of a trademark in an expressive work does not constitute infringement unless the use has absolutely no "artistic relevance" to the underlying work, or, if it does have some artistic relevance, it "explicitly misleads" the public as to the source or content of the work.[23]

The bar for meeting the first prong requirement at an extremely minimal level, making it easy for most expressive works to satisfy it. Courts have ruled that the level of artistic relevance merely needs to be above zero.[24] For example, in a case involving the video game Grand Theft Auto: San Andreas, the creators included a virtual strip club called the "Pig Pen," which closely mocked a real-world club called the "Play Pen". The court applied the Rogers test and found that incorporating the modified logo into the game had artistic relevance because it helped create a cartoon-style parody of East Los Angeles.[25] Because the standard is so permissive, most artistic uses easily pass this first hurdle.

The second prong asks whether the use is explicitly misleading. This means that an expressive work loses its First Amendment protection if it induces the public to falsely believe that the trademark owner created, endorsed, or sponsored the work. To evaluate this, courts often look at traditional likelihood of confusion factors, but they require a particularly compelling showing of confusion to outweigh free speech interests.

However, the broad protection offered by the Rogers test was recently narrowed by the United States Supreme Court in ***Jack Daniel's Properties, Inc. v. VIP Products LLC***.[26] In this case, a company created a dog toy called "Bad Spaniels" that mimicked the shape and label of a Jack Daniel's whiskey bottle, replacing the brand's slogans with bathroom humor. While lower courts had protected the toy as an expressive parody under the Rogers test, the Supreme Court

[22] *Rogers v. Grimaldi*, 695 F. Supp. 112 (S.D.N.Y. 1988).
[23] Morgan Garces, *Bad Spaniels or Bad Trademark Law? How a Supreme Court Decision Narrows the Parody Defense*, Univ. Miami L. Rev. (Feb. 13, 2025), https://lawreview.law.miami.edu/bad-spaniels-or-bad-trademark-law-how-a-supreme-court-decision-narrows-the-parody-defense/.
[24] *E.S.S. Ent. 2000, Inc. v. Rock Star Videos*, Inc., 547 F.3d 1095, 1100 (9th Cir. 2008).
[25] James G. Gatto, D. Benjamin Esplin & Justin A. Pan, *Trademark Claims Against Virtual World Strip Club Denied on 1st Amendment Grounds*, at 5 (Pillsbury Winthrop Shaw Pittman LLP Jan. 20, 2009).
[26] *Jack Daniel's Props., Inc. v. VIP Products LLC*, 599 U.S. 1, 2–3 (2023).

ruled that the Rogers test does not apply at all when the alleged infringer uses the trademark as a "*designation of source for the infringer's own goods*".[27] In other words, if a creator uses a brand's recognizable features as a trademark to sell their own competing commercial products, they cannot hide behind the First Amendment to avoid traditional infringement and dilution scrutiny. This landmark decision has forced creators to walk a much finer line, as a successful parody must now balance its humor against its potential to serve as a commercial source identifier.

EU's transatlantic divergence from Rogers

The European Union approaches the balance between trademark protection and freedom of expression quite differently. Unlike the American system, which relies heavily on the First Amendment and judicially created tests, the EU balances these interests through specific statutory limitations and exceptions codified in the European Union Trade Mark Regulation (EUTMR)[28] and the Trade Mark Directive (TMD)[29]. *Article 14* of the EUTMR explicitly limits a trademark owner's exclusive rights, allowing third parties to use a protected mark in specific circumstances.[30]

One such defense is descriptive use, which allows individuals to use a trademark to describe the kind, quality, intended purpose, or other characteristics of their own goods or services. Another key defense is referential use, which permits the use of a trademark when it is necessary to identify or refer to the trademark owner's goods or services. This is often used by third parties to indicate that their product is an accessory or a spare part compatible with a famous brand.[31]

Crucially, both of these EU defences are subject to a strict overarching requirement: the third party must use the mark "*in accordance with honest practices in industrial or commercial matters*". The concept of honest practices requires the user to act fairly in relation to the

[27] John R. Vile, *Jack Daniel's Properties, Inc. v. VIP Products LLC (2023), First Amendment Encyclopedia* (July 18, 2023), https://firstamendment.mtsu.edu/article/jack-daniels-properties-inc-v-vip-products-llc/.
[28] Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trade Mark, 2017 O.J. (L 154).
[29] Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 Dec. 2015 to Approximate the Laws of the Member States Relating to Trade Marks, 2015 O.J. (L 336).
[30] EUTMR, *supra* note 28, art. 14 (*"Limitation of the effects of an EU trade mark"*).
[31] Til Todorski, *"Due Cause" as a Mechanism to Safeguard Fundamental Rights Under EU Trade Mark Law* 32 (LL.M. Thesis, Stockholm University 2024).

legitimate interests of the trademark owner.[32] A use fails the honest practice test if it gives the false impression that there is a commercial connection between the third party and the trademark owner, if it takes unfair advantage of the mark's distinctive character, or if it discredits and denigrates the famous brand.[33] This standard often places the burden on the artist or user to prove they complied with commercial fairness, which can be a difficult hurdle for creators who are not familiar with industry norms.

Parody in the EU presents a particularly complex challenge. While copyright law in the EU contains a specific statutory exception for parody, there is no explicit equivalent in EU trademark law. Instead, artists seeking to defend a trademark parody must rely on the broader right to freedom of expression, guaranteed by the Charter of Fundamental Rights of the European Union.[34] Because parody is not an autonomous statutory defense in trademark disputes, European courts often perform an internal balancing act. They evaluate whether the parody is justifiable under the "due cause" exception, which allows third parties to use a famous mark without liability if they have a legitimate reason that outweighs the trademark owner's interests. To establish *due cause* through freedom of expression, a parody must typically evoke the original work while being noticeably different, and it must constitute an expression of humor or mockery.[35] However, if the parody is highly commercial or severely tarnishes the brand, EU courts are likely to rule that the artist acted without due cause and violated honest practices.

The Chilling Effect of Expansive Online Contacts

Beyond the substantive defences of free speech and parody, the digital age has introduced a profound procedural threat to expression, widely known as the '***chilling effect***.' The chilling effect occurs when individuals self-censor and refrain from exercising their lawful right to free speech because they fear the unpredictable and ruinous consequences of the legal process itself.[36] In the era of Web 3.0 and global social media, the internet has made communication

[32] *Ibid* at 33, 34.
[33] Alexandra Louise Tiedeman, *To what extent is the fundamental right of artistic expression balanced against the protection of trademark rights in the NFT domain versus in the physical environment in the US and the EU?* 23–24 (LL.M. Thesis, Tilburg University 2024).
[34] Martins, *supra* note 14, at 165.
[35] Leonardo Machado Pontes, Trademark and Freedom of Speech: A Comparison Between the U.S. and the EU System in the Awakening of Johan Deckmyn v. Helena Vandersteen, WIPO Doc. No. WIPO/IPL/GE/15/T3, at 44 (2015) https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ipl_ge_15/wipo_ipl_ge_15_t3.pdf.
[36] J. Townend, *Defamation, Privacy & the "Chill": A Socio-Legal Study of the Relationship Between Media Law and Journalistic Practice in England and Wales*, 2008–13 47 (Ph.D. thesis, City, Univ. of London 2014).

entirely borderless, yet our legal systems remain strictly territorial. This mismatch has turned basic online interactions into potential legal traps.

A major driver of this modern chilling effect is how courts determine personal jurisdiction in cases involving online speech. Under established due process principles, courts have historically been permitted to assert jurisdiction over non-resident defendants only when those defendants have purposefully established *'minimum contacts*' with the forum state.[37] However, the viral nature of the internet means that a post written in a local living room can instantly reach a national or global audience without the speaker's direct intent.[38] Rather than updating these rules to protect digital speakers, several courts have begun treating the actual content of the speech, such as, conversational tools and geographic references as the necessary minimum contacts to establish jurisdiction.

Under this content-focused approach, courts look at whether an internet user utilized platform features like an "@" tag or a mention to interact with a specific entity. For example, the US's Sixth Circuit Court of Appeals has treated the act of tagging a company's social media handle as the functional equivalent of sending a direct letter or making a phone call into the state where that company is located.[39] In ***Majumdar v. Fair***, a court ruled that a defendant could be sued in Illinois simply because she tagged a university's official handle in her tweets, declaring that the tagging was an intentional choice to direct allegations into the state.[40] Consequently, the determination of whether a user can be dragged into a distant court can hinge entirely on the inclusion or omission of a single "@" symbol.

This judicial approach creates a severe chilling effect on free speech. Tagging and mentioning are fundamental conversational tools designed to engage audiences and contribute to public discourse; they are rarely intended as deliberate legal actions directed at a specific geographic

[37] Brian D. Wassom, *Socializing Over State Lines: Social Media as a Basis for Personal Jurisdiction*, Warner Norcross + Judd LLP (Apr. 25, 2012), https://www.wnj.com/updates/socializing-over-state-lines-social-media-as-a-basis-for-personal-jurisdiction/.
[38] Devanshi Patel-Martin, *Personal Jurisdiction in the Shadow of the First Amendment*, 114 Calif. L. Rev. 247, 249 (2026).
[39] *Ibid* at 287.
[40] *Majumdar v. Fair*, No. 21 C 928, slip op. (N.D. Ill. Oct. 19, 2021). *("Defendant's distinction makes no difference. The fact that a Twitter mention or Facebook tag is a means of addressing a public rather than private communication to a particular user does not make it any less an intentional, direct contact. When a Facebook user is tagged or a Twitter user is mentioned, the user receives a notification directing his or her attention to the post, just as an email user receives a notification when he or she receives an email. Defendant does not dispute that numerous courts have found emails to people in the forum state to be relevant contacts for jurisdictional purposes.")*

territory. By treating these everyday digital features as jurisdictional hooks, courts expose ordinary users to the threat of defending lawsuits thousands of miles from home simply for participating in an online conversation.[41] The burden of fighting a lawsuit in a foreign jurisdiction can be financially and emotionally devastating.

When the jurisdictional trigger is so unpredictable that users cannot know which casual tags might expose them to distant litigation, the legal procedure itself operates as a tool of suppression. The threat of SLAPP suits (Strategic Lawsuits Against Public Participation) relies precisely on this dynamic, utilizing the heavy cost and stress of the legal process to intimidate critics into silence.[42] If speakers must choose between expressing their opinions and risking bankruptcy in a remote courtroom, most will choose to stay silent. Therefore, legal scholars argue that courts must integrate First Amendment values directly into the jurisdictional analysis, ensuring that the procedural rules of the digital age do not inadvertently destroy the uninhibited, robust debate that free speech laws are meant to protect.

THE JURISDICTIONAL FRONTIER: LOCALIZING INFRINGEMENTS

Under this doctrine, the legal protection afforded to IP rights, including both trademarks and copyrights extends no further than the sovereign borders of the nation that originally conferred those rights. This principle establishes that intellectual property rights, such as trademarks and copyrights, are strictly limited to the physical territory of the specific state or country that granted them. In the physical world, this framework is logical and relatively easy to enforce. A trademark registered in France, for example, only provides protection and legal rights within French borders. However, the internet and the rapidly expanding metaverse operate quite differently. These digital environments are fundamentally borderless and global by design,. When an unauthorized user creates a digital asset that infringes on a famous brand within a virtual world, that asset can instantly be viewed, interacted with, and purchased by users across the globe,. This creates a severe legal friction between borderless technology and territorial laws. When an infringement occurs, courts face a massive challenge in localizing the dispute to determine which country's laws apply and which court actually has the authority to hear the

[41] See *Courtney Love Cobain v. Gordon & Holmes*, BC525857 (Cal. Super. Ct. Oct. 25, 2013);
Martha Neil, Defense Verdict for Courtney Love in "Twibel" Case Brought by Her Former Lawyer, A.B.A. J. (Jan. 27, 2014),
https://www.abajournal.com/news/article/defense_verdict_for_courtney_love_in_twibel_trial_brought_by_her_former_law. *("She told the jury she had meant to send a private message to Holmes on Twitter but accidentally made it public and then promptly deleted it…")*

[42] *SLAPP Suit*, Legal Info. Inst. (Cornell L. Sch.), https://www.law.cornell.edu/wex/slapp_suit.

case.

Localizing through Causal event.

To solve this problem and determine proper jurisdiction, legal systems have developed and evaluated three main approaches for localizing online disputes. The first method is known as the ***causal event approach***.[43] This method focuses on the exact physical location where the wrongdoer initiated the harmful conduct. Under this approach, a court might look at where the defendant is officially established, where they live, or where they physically pressed the button to upload the infringing content to a network,. While this seems like a straightforward way to anchor a digital act to a physical location, it has significant practical shortcomings. In the modern digital landscape, discovering the origin of a causal event is incredibly difficult. An infringer might be completely anonymous, masking their location through advanced technology, or the virtual world might be hosted on a decentralized network scattered across multiple international servers.[44]

Localizing through Accessibility

Because finding the exact origin of an upload can be nearly impossible, some courts have relied on a second method called the ***accessibility approach***.[45] This method determines jurisdiction based simply on whether the infringing digital content can be accessed or viewed within the court's territory. Under this logic, if a user in a specific country can pull up the infringing virtual good on their screen, the courts in that country could claim they have the power to hear the case. However, legal experts and international courts heavily criticize this approach.[46] Because internet content is instantly available worldwide, using mere accessibility as a standard effectively creates universal jurisdiction,. It implies that a digital creator or website operator could potentially be dragged into court in almost any country on Earth, even if they never intended to interact with people living there. This widespread exposure creates a severe chilling

[43] Eleonora Rosati, *The Localization of IP Infringements in the Online Environment: From Web 2.0 to Web 3.0 and the Metaverse*, at 19 (WIPO 2023).
[44] Eleonora Rosati, *The Localization of IP Infringements in the Online Environment: From Web 2.0 to Web 3.0 and the Metaverse*, 18 J. Intell. Prop. L. & Prac. 720, 734 (2023).
[45] Rosati, *supra* note 43.
[46] Geneva Internet Dispute Resolution Policies 1.0, at 4 (Univ. of Geneva 2015), https://geneva-internet-disputes.ch/medias/2016/11/gidrp-1-0-geneva-internet-dispute-resolution-policies-final.pdf. *("This approach should be rejected. It ignores that many globally available websites, such as teen blogs, local and regional businesses and news sites, or personal websites do not seek global attention. It creates a risk of forum shopping and allows any court to enjoy universal jurisdiction over all websites which do not specifically make use of technological ways of filtering users.")*

effect on digital commerce and encourages unfair forum shopping, a practice where plaintiffs search the globe for the court that will give them the most favorable outcome or the highest damages.

Localizing through Targeting

To find a fairer balance, many courts around the world have shifted to a third method, known as the ***targeting approach***.[47] Today, this is widely considered the prevailing and most effective method for localizing online disputes. Instead of looking at mere accessibility, the targeting approach asks whether the infringer purposefully directed their online activity at the consumers of a specific territory.[48] Courts look for concrete, objective evidence of this intention. For example, they will examine if the website or virtual platform uses the local language of that country, accepts the local currency, or uses a specific country's top-level domain name. They also look at whether the platform offers local customer service, outlines specific import duties, or uses specific platform tags and geo-targeted advertising to attract residents of that state,. If these elements are present, the court can confidently determine that the infringer targeted that specific market, making it fair and reasonable to hold them accountable in that jurisdiction.

Contrasting US's Flexibility with EU's Formalism

These localization criteria are applied through formal regulatory frameworks, which operate differently depending on the region. In the United States, jurisdiction over out-of-state or foreign defendants is governed by constitutional due process and the minimum contacts standard,. The US Supreme Court established that subjecting a defendant to proceedings in a remote jurisdiction is permissible only when that defendant has meaningfully engaged with the forum in a way that makes litigation there foreseeable and "*legal process does not offend traditional notions of fair play and substantial justice.*"[49] Over time, this evolved into the requirement of '***purposeful availment***.' This means the defendant must have intentionally exploited the market of the forum state, thereby invoking the benefits and protections of its laws,. American courts routinely emphasize that merely operating a passive website that

[47] Rosati, *supra* note 43.
[48] Rosati, *supra* note 44 at 731.
[49] *Int'l Shoe Co. v. Washington, Officer of Unemployment Compensation & Placement*, 326 U.S. 310, 316 (1945). *("But now that the capias ad respondendum has given way to personal service of summons or other form of notice, due process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.")*

happens to be accessible in a state does not satisfy this *purposeful availment* requirement. Instead, for intentional torts like trademark infringement, courts often apply an "effects test" to see if the defendant's efforts were expressly aimed or purposefully directed at the state, which closely mirrors the targeting approach.[50]

The European Union uses a different, highly codified statutory system to manage cross-border disputes, primarily relying on the Brussels I Recast Regulation and the Rome II Regulation. The Brussels I Recast Regulation is used to determine which specific court has jurisdiction to hear the case. Its general rule states that a defendant should always be sued in the country where they are domiciled. As an exception to the domicile rule, the regulation permits claimants to bring an action before the courts of the jurisdiction in which the damage materialised or is likely to materialise. To determine exactly where this harmful event occurred, European courts increasingly use the targeting approach to see if the infringer directed their commercial activities toward a specific Member State. Once the correct court is established, that court must decide which country's laws to apply to the actual infringement. This is governed by the Rome II Regulation. For intellectual property disputes, Rome II relies on the principle of the country of protection,. This means the applicable law is the law of the country for which the intellectual property protection is claimed.

Ultimately, both the United States and European Union frameworks are working to adapt physical-world rules to the borderless digital economy, striving to ensure that jurisdiction is based on intentional, targeted actions rather than accidental global reach.

ENFORCEMENT CHALLENGES AND PLATFORM LIABILITY

Behind the scene (screen)?

When brands try to enforce their intellectual property rights in the metaverse, their first major hurdle is simply identifying the wrongdoer. In the physical world, law enforcement can track down a factory making counterfeit goods. In the virtual world, users interact through digital avatars and often hide behind fake names or pseudonyms,. This makes it incredibly hard to

[50]Int'l Trademark Ass'n, *supra* note 6, at 39. *("A consistent view has emerged that the "purposeful availment" prong is not satisfied by merely operating a website accessible in a state. Plixer Int'l, Inc. v. Scrutinizer GmbH, 905 F.3d 1, 8 (1st Cir. 2018) (collecting cases). This is so even if a website is "interactive." See, e.g., be2 LLC v. Ivanov, 642 F.3d 555, 558–59 (7th Cir.2011). Instead, the defendant must have purposefully exploited the market of the forum state, such that it could reasonably expect to be hauled into court in that state. See Plixer Int'l Inc., 905 F.3d at 11.")*

know who is actually operating the avatar. The problem is even worse in decentralized networks. These networks rely on blockchain technology and cryptocurrency wallets for buying and selling virtual goods. A blockchain wallet is identified only by a long public string of numbers and letters, not by a person's real name, home address, or email address. Because these wallets heavily shield the true identities of the users, brand owners face a massive wall of anonymity.[51] Sometimes, a brand must file a special legal claim known as a "John Doe" lawsuit.[52] This is a lawsuit filed against an unknown person, which is used to force cryptocurrency exchanges to reveal the real identity hiding behind the digital wallet. Even then, finding the infringer is a slow and expensive process. Furthermore, many virtual spaces are governed by Decentralized Autonomous Organizations, or DAOs. A DAO has no central boss or corporate headquarters. Instead, it is managed by a scattered community of anonymous users who vote on decisions,. When an infringement happens in a DAO, it is extremely difficult to determine who is legally responsible for the theft.[53]

Who Polices the Metaverse?

Because suing an anonymous avatar is so difficult, intellectual property owners frequently turn their attention to the tech companies that build and run these virtual worlds. Brands want these platform operators to police the metaverse and remove illegal items. To balance the needs of brands and tech companies, lawmakers rely on intermediary liability rules. In the United States, the Digital Millennium Copyright Act[54] (DMCA), known as the DMCA, is the primary law used to manage these digital disputes. The DMCA provides a legal *safe harbor* for online platforms. This means a tech company will not be held legally responsible for the copyright infringements committed by its users, provided the company follows specific rules. The most important rule is the notice-and-takedown system.[55] If a brand owner spots a copied digital item, they must send a formal notice to the platform. The platform must then remove the illegal content quickly to keep its *safe harbor* protection.

[51] Int'l Trademark Ass'n, *Non-Fungible Tokens (NFTs) White Paper*, at 66 (Apr. 4, 2023), https://www.inta.org/wp-content/uploads/public-files/perspectives/industry-research/METAVERSE_REPORT-070323.pdf.
[52] *John Doe Lawsuits for Discovery*, Silver Miller, https://www.silvermillerlaw.com/current-investigations/john-doe-lawsuits-for-discovery/.
[53] Ana Mercedes López Rodríguez, *Consumer Protection in Blockchain-Based Metaverses: A Comparative Study of Cross-Border Legal Gaps and Platform Governance*, 8 Frontiers Blockchain 1675735, 5–6 (2025).
[54] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).
[55] 17 U.S.C. § 512. ("*Limitations on liability relating to material online*")

The European Union takes a similar but updated approach through the Digital Services Act[56], or DSA. The DSA was created to modernize older internet laws and make the digital space safer for everyone. Like the American system, the DSA offers a *safe harbor* for platforms that simply host content. A metaverse provider is not liable for illegal digital goods if it does not actually know about them. However, once the platform receives a proper notice about the illegal content, it must act rapidly to disable access or remove the item.[57] The DSA also forces platforms to be highly transparent with their users. If a platform removes an item, it must explain exactly why and give the user a fair chance to appeal the decision.[58] While these notice-and-takedown regimes work well on centralized platforms like traditional social media, they face massive technical hurdles in a decentralized metaverse. On a decentralized blockchain network, files are copied and spread across thousands of independent computers. Because the blockchain is designed to be permanent, there is no single central server where a company can simply delete an infringing file. Once a fake virtual item is minted on the blockchain, it is essentially there forever.[59]

Smart Enforcement from Detection to Deletion

Since traditional laws struggle with decentralized technology, brands are increasingly turning to alternative enforcement mechanisms built directly into the software. One of the most effective tools is the use of *smart contracts*. A smart contract is self-executing code embedded within a blockchain that carries out predetermined actions automatically once the agreed-upon triggering conditions have been satisfied. Brands can write their trademark and copyright rules directly into these smart contracts.[60] For example, a brand can program a smart contract to verify if a seller is an authorized dealer before allowing a virtual sale to go through. If an unauthorized user tries to sell a fake digital item, the smart contract will automatically block the transaction. In addition to smart contracts, blockchain technology provides strong authentication. It creates an unchangeable, permanent record of who truly owns a digital asset. This allows buyers to instantly check the history of a virtual good and confirm that it originated

[56] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, 2022 O.J. (L 277).
[57] *Id.* art. 16. (*"Notice and action mechanisms"*)
[58] *Id*. arts. 17, 20. (*"Statement of reason; Internal complaint-handling system"*)
[59] Anthony V. Lupo, James Williams & Dan Jasnow, *Protecting and Enforcing IP Rights in the Metaverse*, Nat'l L. Rev. (Apr. 22, 2022), https://natlawreview.com/article/protecting-and-enforcing-ip-rights-metaverse.
[60] Bao Tran, *The Role of Smart Contracts in Enforcing Trademark Rights in the Metaverse*, PatentPC (Mar. 15, 2026), https://patentpc.com/blog/the-role-of-smart-contracts-in-enforcing-trademark-rights-in-the-metaverse.

from the official brand, effectively stopping counterfeiters in their tracks.[61]

Artificial intelligence is another powerful weapon for enforcing intellectual property rights in the metaverse. Virtual worlds are massive, making it impossible for human workers to manually search every digital store or gaming environment for stolen logos. To solve this, brands use AI algorithms to conduct real-time monitoring of the digital landscape. These AI tools can scan virtual spaces, non-fungible token marketplaces, and social platforms continuously. They use advanced image, text, and sound recognition to identify unauthorized uses of a brand's assets.[62] For instance, if a user uploads a digital jacket featuring a slightly altered luxury logo, the AI can detect the visual similarity and instantly flag the item. Once an infringement is detected, the AI system can automatically send a takedown notice to the platform or even trigger a smart contract to halt the sale. This automated detection saves brands significant time and money while keeping their virtual presence secure.[63]

Finally, when brands are forced to rely on the court system to stop fast-moving digital infringements, they are increasingly seeking dynamic injunctions. In a traditional lawsuit, a judge issues an order to stop a specific, known illegal activity. However, internet pirates and digital counterfeiters move incredibly fast. If a court orders one fake virtual store to shut down, the infringer will often create a new mirror site under a different name just minutes later. This creates a frustrating game of whack-a-mole for brand owners. Traditional dynamic injunctions were insufficient because they only addressed existing pirated content or mirror websites, failing to protect future infringing works. Recognizing this limitation, the Delhi High Court in ***Universal City Studios LLC & Ors. v. Dotmovies.baby & Ors***[64] introduced the "dynamic+" injunction to proactively protect newly released films from piracy. Dynamic+ injunctions solve this problem by adapting to the infringer's new tactics. Instead of requiring the brand to file a new lawsuit for every new fake website, a dynamic injunction allows the court to order intermediaries, like internet service providers or platform hosts, to pre-emptively block any

[61] Andrew N. Choi & Cindy A. Gierhart, *Intellectual Property Enforcement in the Metaverse, Part 3: Bigger-Picture Considerations*, Holland & Knight (Oct. 18, 2022), https://www.hklaw.com/en/insights/publications/2022/10/intellectual-property-enforcement-in-the-metaverse-part-3. (See under heading: *"Traceability"*)

[62] Koushik Banerjee, Tech Meets Trademarks: AI, Blockchain, and NFTs in Brand Protection for 2025, De Penning & De Penning (Dec. 12, 2025), https://depenning.com/blog/tech-meets-trademarks-ai-blockchain-and-nfts-in-brand-protection-for-2025/. (See under heading: "*AI in Trademark Enforcement"*)

[63] Bao Tran, *AI-Driven Trademark Monitoring: Catching Infringements Early*, PatentPC (Mar. 3, 2026), https://patentpc.com/blog/ai-driven-trademark-monitoring-catching-infringements-early. (See under heading: *"Saving Time and Reducing Costs"*).

[64] *Universal City Studios LLC v. Dotmovies.baby*, CS(COMM) 514/2023, order dated Aug. 9, 2023 (Del. High Ct.).

future mirror sites. This proactive legal tool allows brands to act swiftly and decisively, lifting the veil of anonymity and stopping digital infringements before they can spread further across the metaverse.

CONCLUSION

The evolution from the conventional internet toward Web 3.0 and immersive virtual environments opens remarkable new avenues for social interaction and cross-border commercial activity. However, as this research paper has shown, this massive digital evolution completely disrupts our traditional intellectual property frameworks. For centuries, our legal systems have relied heavily on physical borders and the strict principle of territoriality to protect creators and famous brands. The metaverse changes all of this. It operates as a borderless global network powered by advanced blockchain technology, virtual reality, and decentralized communities. Because virtual assets move instantly across international lines, and because users often hide behind anonymous digital avatars, it is incredibly difficult to figure out where a legal infringement happened. Furthermore, it is very hard to determine which country has jurisdiction over a dispute. Ultimately, our current laws were built for physical goods in a physical world. They struggle deeply to govern a decentralized, intangible digital space.

To survive and thrive in this new environment, brand owners must take strategic and proactive steps. First, businesses should not wait for an infringement to happen before they take action. They must pursue pre-emptive trademark registration for their digital goods and virtual services. By filing trademark applications early in specific digital categories, brands establish a strong legal shield for their virtual items. Second, brand owners must focus on the careful drafting of licensing agreements. When companies partner with digital creators, game developers, or metaverse platforms, these contracts must clearly state exactly how their intellectual property can be used in virtual spaces. Using smart contracts on the blockchain can also help automate these agreements and enforce the rules instantly. Finally, active digital monitoring is absolutely essential. The metaverse is too vast for human workers to manually check every corner. Brands need to use advanced artificial intelligence tools and digital watch services to constantly scan virtual worlds and non-fungible token marketplaces. This active monitoring ensures they can spot and stop unauthorized uses of their logos before major damage occurs.

When disputes inevitably arise, traditional court litigation often gets bogged down in complex jurisdictional battles. Therefore, Alternative Dispute Resolution, such as arbitration and mediation, offers a highly effective way to handle cross-border intellectual property infringements in the metaverse. Arbitration allows parties to choose a neutral forum with specialized technical experts, and international arbitration awards are much easier to enforce across borders than traditional court judgments, largely thanks to international treaties like the New York Convention.[65] Furthermore, the metaverse has given rise to innovative, blockchain-based dispute resolution systems. Platforms like Kleros and Aragon use decentralized justice, where crowdsourced, anonymous jurors review digital evidence and vote on a dispute.[66] Crucially, this arbitration process can be linked directly to a smart contract, which can automatically execute the tribunal's award by instantly freezing an infringing asset or transferring a digital token without ever needing a traditional court.[67]

While individual brands can take these protective steps, the global legal community must also take bold action. We urgently need global legal harmonization to solve the core paradox of the metaverse. Relying on a fractured patchwork of different national laws is simply no longer effective for a worldwide digital economy. The legal and technological communities must work together to build a unified "meta-jurisdiction" that provides clear, shared rules for resolving digital disputes. To successfully bridge the massive gap between strict territorial laws and the completely borderless metaverse, international organizations must step in. We need updated international treaties, such as modern updates to the World Intellectual Property Organization treaties or the Berne Convention, to explicitly cover virtual spaces and digital assets. By creating a unified global legal framework, we can fully protect the rights of creators and brands while allowing the metaverse to grow as a safe, innovative, and thriving digital frontier.

[65] Convention on the Recognition and Enforcement of Foreign Arbitral Awards art. [article], June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 3.

[66] World Intell. Prop. Org. (WIPO), Blockchain Technologies and IP Ecosystems: A WIPO White Paper 47 (2020).

[67] Tatevik Karapetyan, The Future of Justice: Enforcing Online Arbitration Awards, ITA in Rev., Vol. 7, Issue 3 (2025), https://itainreview.org/articles/2025/Vol7/Issue3/the-future-of-justice-enforcing-online-arbitration-awards.html. *("In the context of emerging technologies, artificial intelligence (AI) and smart contracts present both challenges and opportunities. AI tools can assist in creating efficient dispute resolution processes and in predicting the outcome of proceedings, which can streamline the enforcement of awards."*)