The Trademark Reporter®

BACK TO THE FUTURE WITH BLOCKCHAIN DOMAIN NAMES: TOWARD A GLOBAL POLICY TO FIGHT CYBERSQUATTING IN WEB 3.0

By Vera Glonina[*]

TABLE OF CONTENTS

* Associate, Leason Ellis LLP, Member, International Trademark Association.

INTRODUCTION

The development of blockchain technologies is changing the world by introducing new systems and opportunities. In particular, blockchain technology is a crucial component of Web 3.0, a new generation of the Internet, incorporating concepts such as decentralization, smart contracts, and digital identity.[1] Some experts state that Web 3.0 is the "read/write/own" upgrade to the Internet, insofar as prior iterations of the web allowed people to read things on the Internet, then to write things on the Internet, and now Web 3.0 offers the ability to own things too.[2] According to Straits Research, "[t]he global web 3.0 blockchain market size was valued at USD 1890 million in 2021. It is estimated to reach an expected value of USD 52890 million by 2030 at a CAGR of 44.8% during the forecast period (2022–2030)."[3]

At the heart of Web 3.0 are blockchain domain names ("BDNs"), domain names based on blockchain technologies, and their potential to revolutionize the way we interact with the Internet is a hot topic. For example, during the international Domain Days Dubai 2023 conference, held in Dubai, United Arab Emirates, in November 2023, Web 3.0 technologies and BDNs were actively discussed.[4] In particular, the attendees discussed "the growth and future web3 domains and the vision of a decentralized, blockchain-powered Internet."[5] During the Dominion 2024 The Future of Web3 Identity & Internet Domains conference, held in April 2024, representatives of the Web 3.0 company D3 Global Inc. stated that it was expected to "onboar[d] the next *billion* [Web3] users" and that necessitated "creating a world in which the Web2 that we know and regularly interact with, is integrated with the technologies that Web3 and the blockchain can offer."[6]

---

1 *What is Web3?*, McKinsey Blog, McKinsey (Oct. 10, 2023), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3.

2 Dan Ashmore, Michael Adams, *A Brief History Of Web 3.0*, Forbes Advisor (Oct 17, 2023, 4:52 AM), https://www.forbes.com/advisor/investing/cryptocurrency/what-is-web-3-0.

3 *Global Web 3.0 Blockchain Market Size is Estimated to Reach USD 52890 million by 2030, Growing at a CAGR of 44.8%: Straits Research*, Finance.Yahoo (Dec. 20, 2023), https://finance.yahoo.com/news/global-3-0-blockchain-market-140500255.html?guccounter=1.

4 *Domain Days conference kicks off today in Dubai*, MENAFN (Nov. 2, 2023), https://menafn.com/1107357177/Domain-Days-conference-kicks-off-today-in-Dubai.

5 *Embracing Web3: Freename's Experience at Dubai Domain Days*, Freename (Nov. 9, 2023), https://freename.io/embracing-web3-freenames-experience-at-domain-days-dubai; *see also Wrapping Up Domain Days Dubai 2023: A Resounding Success for Dubai Blockchain Center*, Dubai Blockchain Center (Nov. 3, 2023), https://blockchaincenter.ae/2023/11/03/wrapping-up-domain-days-dubai-2023/.

6 Shane Layman, *Web3 Innovation: Interoperability With Web2 Domains*, Markmonitor (May 13, 2024), https://www.markmonitor.com/blog/web3-interoperability-with-web2-domains/ [hereinafter *Web3 Innovation*].

BDNs are a new and evolving technology. However, BDNs present numerous challenges from a legal perspective, including challenges related to trademark law. Web 3.0 providers, similar to most Web 2.0 domain name providers, allow users to register BDNs containing designations identical or similar to registered trademarks, including various well-known trademarks. However, there are no specific verification or enforcement mechanisms applicable to BDNs, which creates additional challenges. For example, in the recent high-profile *Hermes International et al. v. Rothschild* case regarding the MetaBirkins project involving virtual versions of Hermes BIRKIN handbags, Hermes asserted numerous causes of action in the United States District Court for the Southern District of New York, and asked for the traditional Web 2.0 domain name metabirkins.com, as well as "any ENS domains [a type of BDN] containing the BIRKIN mark," to be transferred to Hermès.[7] In contrast, the possible enforcement options with respect to BDNs are significantly more complicated.

This article focuses on worldwide trademark protection in Web 3.0, including within BDN systems such as Ethereum and Unstoppable. Unlike traditional ICANN-managed domain names, BDNs are decentralized and operate within an alternative domain name system, which is independent of the ICANN network and is not subject to the ICANN rules, including the Uniform Domain Name Dispute Resolution Policy ("UDRP"). In other words, BDNs are not subject to the transfer and cancellation remedies available to trademark owners under UDRP or other ICANN-coordinated procedures. Also, BDNs might be outside of national anticybersquatting laws and regulations. For example, the applicability of the Anticybersquatting Consumer Protection Act ("ACPA") to BDNs remains debatable and not explicitly confirmed by any court decision.

This article explores the practical trademark-related challenges resulting from the rise of various decentralized domain name systems. It proposes certain regulatory mechanisms to fight trademark infringement in Web 3.0, including potential amendments to the ACPA and national anticybersquatting laws of other countries, and creating a global UDRP-like system for resolving disputes involving BDNs.

Part I lays out the current U.S. and certain foreign regulatory frameworks aimed to ensure trademark protection in the digital era, in particular, the protection of trademark owners against cybersquatting, i.e., unlawful registration and use of domain names containing trademarks. Part II discusses the current legal and

---

7 Hermès Memorandum of Law in Support of Plaintiffs' Motion for Permanent Injunction, Hermes Int'l et al. v. Rothschild, No. 1:22-cv-00384, CourtListener, https://storage.courtlistener.com/recap/gov.uscourts.nysd.573363/gov.uscourts.nysd.573363.166.0.pdf, Doc. 166, at *18 (S.D.N.Y. Mar. 20, 2023).

practical challenges caused by the rise of Web 3.0 and various alternative domain name systems, focusing on BDNs. This part analyzes some U.S. and foreign examples of cybersquatting as part of NFT-based projects and the registration system of BDNs. This article also presents an overview of the shortcomings of the current trademark protection system in Web 3.0, focusing on the lack of proper mechanisms to address cryptosquatting, i.e., unlawful registration and use of BDNs containing trademarks. Part III presents potential solutions to ensure trademark protection in Web 3.0, including creating an international UDRP-like system for BDNs.

PART I. EXISTING TRADEMARK PROTECTION FOR DOMAIN NAMES IN WEB 2.0

A. Domain Names and Cybersquatting: Pre-Internet Framework and Landmark Cases

The Internet's domain-name system ("DNS") is the system that allows users to "refer to web sites and other resources using easier-to-remember domain names (such as "www.icann.org") rather than the all-numeric IP addresses (such as "192.0.34.65") assigned to each computer on the Internet."[8] Domain names are an essential part of the so-called Web 2.0, the current Internet framework.[9]

DNS "can be described as comparable to a phone book of the internet. Its purpose is to direct a user to the intended website and resolve the input of an address to an output on the internet."[10] In this regard, domain names can be described as "a street address for getting postal mail," still requiring something like "a building or post office box to receive letters or packages" to operate websites and otherwise use the domain name.[11]

There are various levels and types of domain names. Some experts describe the DNS as "a tree-like hierarchy."[12] At the highest

---

8 *Top-Level Domains (gTLDs)*, ICANN, https://archive.icann.org/en/tlds/#:~:text=The%20right%2Dmost%20label%20in,%22)%2C%20and%20so%20on (last visited Aug. 14, 2024).

9 *See, e.g.*, Darcy DiNucci, *Fragmented Future*, Design & New Media 32 (1999), https://perma.cc/WR6L-YNE2; *see also* Tim O'Reilly, *Web 2.0 and the Emergent Internet Operating System*, O'Reilly Media, Inc., https://www.oreilly.com/tim/p2p/ (last visited Aug 14, 2024).

10 Georgia Osborn and Nathan Alan, *Web 3 disruption and the domain name system: understanding the trends of blockchain domain names and the policy implications*, 8 Journal of Cyber Policy 142, 142 (2023), https://doi.org/10.1080/23738871.2023.2294759 [hereinafter *Web3 disruption*].

11 About Domain Names, ICANN (last visited Aug. 16, 2024).

12 *Top-Level Domains (gTLDs)*, *supra* note 8.

level is the root domain, which "is at the apex of the domain name hierarchy."[13]

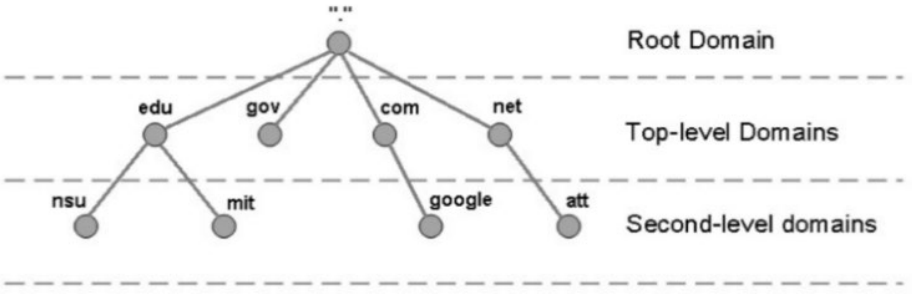

Image source:
https://raventools.com/marketing-glossary/root-domain/

Next, labels in a domain name like .com, .net, and .us are referred to as the "top-level domain" ("TLD"), which are further divided into second-level domains, third-level domains, etc.[14]

TLDs include different types such as (i) generic TLDs ("gTLDs"), the most common and unrestricted global domain names without any territorial limits (e.g., .com, .net, and .org), and (ii) country code top-level domains ("ccTLDs"), TLDs specifically designated for a particular country, sovereign state, or autonomous territory for use to service their community. ccTLDs may or may not be available for registration by a foreign national as determined by local policies (e.g., .uk, .au, and .us.).[15]

Second-level domains are typically used to identify an organization or business (e.g., "google" in the domain name google.com).[16] There might also be certain subdomains (i.e., third-level, forth-level, etc. domain names) that generally help to organize and navigate different sections of a website.[17] Subdomains appear to the left of the second-level domain name and can be easily created within a domain registrar (e.g., test.google.com).[18]

The responsibility for operating each TLD (gTLDs or ccTLDs, including maintaining a registry of the second-level domains within the TLD) is delegated to a particular organization.[19] These

---

13 Matt Conran, *DNS Tree Structure*, *supra* note 12.

14 *Id.*

15 *See* Anne Gilson LaLonde, Gilson on Trademarks § 7A.02 (2023).

16 *Id.*

17 Matt Conran, *DNS Tree Structure*, *supra* note 12.

18 *See* Colleen Branch, *What is a Subdomain? Definition & Examples*, Namecheap Blog (Aug. 24, 2020), https://www.namecheap.com/blog/what-is-a-subdomain-dp.

19 *Top-Level Domains (gTLDs)*, *supra* note 8.

organizations are referred to as "registry operators," "sponsors," or simply "delegees."[20]

Historically, the domain name registration process was developed and managed by the Internet Assigned Numbers Authority ("IANA") group.[21] In 1998, the Internet Corporation for Assigned Names and Numbers ("ICANN") received primary control over the domain name system.[22] Since then, ICANN has been leading the management and oversight of the domain name registration process, and domain names governed by ICANN can be described as "ICANN-coordinated" or "Web 2.0."[23]

Web 2.0 domain names are delegated and registered through the complex system of organizations accredited by ICANN (known as ICANN-accredited registrars).[24] The ICANN-accredited registrars check if a domain name is available and can reserve and create a record with the domain name registrant's information.[25] In most cases, domain names are distributed on a first-come-first-serve

---

20 *Id.*

21 *The History of ICANN*, Int'l Corp. for Assigned Names & Numbers, https://www.icann.org/history (last visited Aug. 14, 2024).

22 *Id.*

23 *See* Alain Durand, *Challenges with Alternative Name Systems*, ICANN (Apr. 27, 2022), https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf [hereinafter *Challenges with Alternative Name Systems*] (stating that "Web2 (or Web 2.0) is the web as it is known today. Web3 is an idea to make the web completely decentralized, building it on a set of tools like blockchain, blockchain-based naming systems, and a distributed storage solution such as the Interplanetary File System (IPFS), a peer-to-peer hypermedia protocol.") As for the historic background, ICANN directly managed IANA from 1998 through 2016, when the contract between two organizations expired. IANA's operation was transferred to Public Technical Identifiers (PTI), an affiliate of ICANN that operates IANA today. See *About the IANA stewardship transition*, IANA, https://www.iana.org/help/pti-transition (September 30, 2016). As of March 2024, IANA is responsible for Root Zone Management (i.e., the process of assigning the operators of top-level domains, such as .uk and .com, and maintaining their technical and administrative details), including maintaining of the Root Zone Database. *See Root Zone Management*, IANA, https://www.iana.org/domains/root (last visited Aug. 14, 2024).

24 *See Registering Domain Names*, ICANN, https://www.icann.org/resources/pages/register-domain-name-2017-06-20-en (last visited Aug. 14, 2024). ("Domain names under generic Top-Level Domain Names (gTLDs) may be registered with one of more than two thousand ICANN-accredited registrars, or their resellers. Registrars are accredited by ICANN organization and certified by the registries to sell domain names. They are bound by the Registrar Accreditation Agreement (RAA) with ICANN organization, and by their agreements with the registries. Resellers are organizations affiliated with or under are under contract with registrars to sell domain names and other services offered by the registrar such as web hosting or email mailboxes. Resellers are bound by their agreements with the registrars whose services they sell and are not accredited by ICANN organization. The registrars remain responsible and accountable for all domain names sold by their resellers. ICANN organization maintains a list of current ICANN-accredited registrars on our website. Domain name registrations under country-code Top-Level Domain Names (ccTLDs) can be made through the ccTLD operators.")

25 *See id.*; *see also Registering Domain Names,* ICANN, https://www.icann.org/resources/pages/register-domain-name-2017-06-20-en (last visited Aug. 14, 2024).

basis to whoever registers a domain name first.[26] In general, it is a fast and user-friendly process. However, this relatively easy registration process has its drawbacks, including registration and use of domain names with the intent of profiting from the goodwill of someone else's trademark (i.e., cybersquatting).[27] Cybersquatting encompasses "a series of practices plaguing trademark owners," that might vary from the most common cases when a cybersquatter "registers a domain name including a well-known trademark for the purpose of selling the name to the trademark owner," to such practices as "typosquatting" (i.e., registration of misspellings of a trademark as a domain name in order to direct those who misspell a domain name to a different website) and "cyberpirating" (i.e., use of the goodwill of the trademark to lure web users to a different site by redirecting or connecting ad revenue).[28] Some experts also separately distinguish "anticipatory cybersquatting," as the "practice of registering domain names with minimal present value in the hopes that these names will become desirable, and therefore increasingly valuable, in the future."[29]

In the 1990s and early 2000s, many U.S. and foreign courts struggled with cybersquatting. An illustrative example is the group of cases involving Dennis Toeppen, who registered numerous domain names containing famous trademarks and company names.[30] Mr. Toeppen did not sell anything on these websites, but instead wanted to sell the domain names themselves to companies with genuine commercial interests in those domain names.[31] Courts analyzed these cases using pre-Internet trademark legislation like the Federal Trademark Act of 1946 and the Federal Trademark Dilution Act of 1995, although neither directly addresses

---

[26] *FAQs for Registrants: Domain Name Renewals and Expiration*, ICANN, https://www.icann.org/resources/pages/domain-name-renewal-expiration-faqs-2018-12-07-en (last visited Aug 14, 2024). The exceptions can be made for certain "reserved" names (e.g., .gov) and ccTLDs in accordance with the registrar's policies. *See, e.g.*, *Domain requirements*, https://get.gov/domains/requirements/.

[27] *See* J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition, § 25A:48 (5th ed. 2024) ("A 'cybersquatter' is a person who knowingly obtains from a registrar a domain name consisting of the mark or name of a company for the purpose of ransoming the right to that domain name back to the legitimate owner for a price.").

[28] *Liability Under the ACPA: A More Effective Approach to Deterring Cybersquatting at Its Source*, 22 Roger Williams U. L. Rev. 327, 330 (2017); *see also* Terese L. Arenth, *Trademark Protection in the Digital Age: Protecting Trademarks from Cybersquatting*, Bus. Law Today (June 2019), https://www.americanbar.org/groups/business_law/resources/business-law-today/2019-june/trademark-protection-in-the-digital-age/?login.

[29] Tamara Michelle Kurtzman, *Cyber Center: The Continued Hijacking and Ransoming of the Domain Name System by Modern-Day Corporate Privateers Bus. Law Today* (June 20, 2016), https://www.americanbar.org/groups/business_law/resources/business-law-today/2016-june/cyber-center-the-continued-hijacking-and-ransoming/.

[30] *See, e.g.*, Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996); *see also* Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).

[31] *Panavision,* 141 F.3d at 1319.

cybersquatting and instead focus on the notion of traditional consumer confusion.[32]

For example, in *Panavision*, the company attempted to register the domain name "panavision.com," but found that Mr. Toeppen had already registered the name.[33] The web page for panavision.com displayed photographs of the City of Pana, Illinois.[34] When the company contacted Mr. Toeppen, he offered to "settle the matter" in exchange for $13,000.[35] After Panavision refused Mr. Toeppen's demand, Mr. Toeppen registered Panavision's other trademark PANAFLEX as the domain name "panaflex.com."[36] As a result, Panavision alleged claims for dilution of its trademark under the Federal Trademark Dilution Act of 1995, 15 U.S.C. § 1125(c) and under the California Anti-dilution statute, Cal. Bus. & Prof. Code § 14330.[37] Panavision also "alleged that Toeppen was in the business of stealing trademarks, registering them as domain names on the Internet and then selling the domain names to the rightful trademark owners."[38] The Federal District Court for the Central District of California and the United States Court of Appeals for the Ninth Circuit ruled in Panavision's favor, holding that "potential customers of Panavision will be discouraged if they cannot find its web page by typing in 'Panavision.com,' but instead are forced to wade through hundreds of web sites," and that "[t]his dilutes the value of Panavision's trademark," even though "Toeppen's conduct varied from the two standard dilution theories of blurring and tarnishment."[39]

Similar precedents exist in numerous foreign jurisdictions, including in both common law and civil law jurisdictions. For example, the first cybersquatting case reported in India is *Yahoo! Inc. v. Akash Arora* (1999), regarding the domain name "yahooindia.com."[40] The defendant had launched a website nearly

---

32 *Id.*; *see also* Jason M. Osborn, Effective and Complementary Solutions to Domain Name Disputes: ICANN's Uniform Domain Name Dispute Resolution Policy and The Federal Anticybersquatting Consumer Protection Act of 1999, 76 Notre Dame L. Rev. 209, 226-227 ("Cybersquatting is generally neither dilution by blurring, nor dilution by tarnishment, the two black letter categories of trademark dilution. As the Panavision court explained, cybersquatters do not "merely 'lessen[] the capacity of a famous mark to identify and distinguish goods or services,' but [rather] eliminate the capacity of . . . [trademarks] to identify and distinguish . . . goods and services on the Internet.").

33 *Panavision*, 141 F.3d at 1319.

34 *Id.* at 1325.

35 *Id.* at 1319.

36 *Id.*

37 *Id.*

38 *Id.*

39 *Id.* at 1327.

40 Shaunak Deshpande, *Cyber Squatting: A study of Legal framework in India*, 3(3) Int'l J. L. Mgmt. & Humanities 1825, 1831 (2020).

identical to the plaintiff's "yahoo.com" website and provided similar services.[41] The defendant argued that because the designation "yahoo" was not a registered trademark in India, defendant's use of "yahoo" was out of the scope of the applicable trademark laws.[42] However, Yahoo managed to obtain a restraining order, the Court observing that defendant's conduct "was an effort to trade on the fame of yahoo's trademark" and that a "domain name registrant does not obtain any legal right to use that particular domain name simply because he has registered the domain name, he could still be liable for trademark infringement."[43]

One of the first cybersquatting disputes in China was the case of *Ikea Co. Ltd. v. Beijing Guo Wang Co. Ltd.* (1999).[44] In this case, Ikea Co. Ltd. owned a registration for its trademark IKEA in China at the time that the defendant registered the domain name "www.ikea.com.cn" in 1997.[45] Ikea sued Guo Wang for trademark infringement.[46] After two years of litigation, the Higher Court ruled in favor of Ikea on the grounds that "the defendant violated the fairness and good faith principles of Article 2 of the UCL and held the defendant liable for unfair competition."[47] The Higher Court recognized that "the defendant's intentional use of the plaintiff's registered mark for commercial purposes indicated that the defendant was trying to prevent the plaintiff from registering "ikea" as its domain name in bad faith."[48]

In jurisdictions in which trademark law did not provide substantial grounds for fighting cybersquatting, companies were often forced to negotiate with cybersquatters and purchase their domain names for an excessive price.[49] Also, in some instances, squatters might preemptively register national trademarks in their own names separately or in addition to registering domain names,

---

41 *Id.*

42 *Id.*

43 *Id.*

44 Mo Zhang, *Governance of Internet Domain Names Against Cybersquatters in China: A Framework and Legal Perspective*, 26 Hastings Int'l & Comp. L. Rev. 51, 68 (2002) (discussing Ikea Co. Ltd. v. Beijing Guo Wang Co. Ltd. (1999)).

45 *Id.*

46 *Id.*

47 *Id.* at 69.

48 *Id.*

49 *See, e.g.*, *Ask HN: how to buy a domain name from a squatter?*, YHacker News (Sept. 30, 2009), https://news.ycombinator.com/item?id=853228 ("I've had a squatter insist that a domain was worth $10,500 just because it's [sic] 'search terms' yielded a paltry 65,000 results. . . ." and "I wanted to buy the .com version of my hn [i.e., Hacker News] handle, but (after contacting them several times), they responded, saying they don't even consider anything less than $50,000."); *see also* Daniel Fisher, *Cybersquatters Rush To Claim Brands In The New GTLD Territories*, Forbes (Feb. 27, 2014), https://www.forbes.com/sites/danielfisher/2014/02/27/cybersquatters-rush-to-claim-brands-in-the-new-gtld-territories/?sh=75da61e73ba9.

which could make the squatting cases even more challenging for the right holders. For example, when the Starbucks coffee chain started its business in Russia in the 2000s, it learned that a trademark squatter had registered STARBUCKS for the purpose of extorting Starbucks. The company that he had set up was a paper company and had no inventory or employees.[50] The squatter demanded $600,000 to sell its rights to the STARBUCKS name and mark to the coffee company.[51] Unlike other companies that preferred to pay thousands of dollars (e.g., Audi) to the same squatter, Starbucks preferred to fight and managed to win after years of litigation.[52]

In this regard, although trademark owners generally managed to prevail on the trademark and fair dealing claims against cybersquatters, such litigation was lengthy, unpredictable, and challenging. Because of this, the need for specific regulations and proceedings to combat these problems became obvious. While the U.S. and numerous foreign jurisdictions took action, in many jurisdictions, the need for such regulations and proceedings remains a pressing issue.

B. The Anticybersquatting Consumer Protection Act (ACPA) and Certain Foreign Anticybersquatting Laws

In 1999–2000, the U.S. Congress enacted several domain-name-specific statutes, most notably the Anticybersquatting Consumer Protection Act ("ACPA"), codified at 15 U.S.C. § 1125(d).[53] In introducing the bill that was the precursor to the ACPA, one Senator stated that cyberpiracy is essentially "fraud, deception, and the bad-faith trading on the goodwill of others . . . . Unauthorized use of others' marks undercuts the market by eroding consumer confidence and the communicative value of the brand names we all rely on."[54] In this regard, the ACPA "enables trademark owners to win the rights to domain names, particularly where the

---

50 Vladimir Biriulin, *Russia: Starbucks wins trade mark battle with One Bucks Coffee*, Managing IP (Aug. 29, 2018), https://www.managingip.com/article/2a5c34h62riq0qwo26u4g/russia-starbucks-wins-trade-mark-battle-with-one-bucks-coffee.

51 *Id.*; *see also* Andrew Kramer, *He Doesn't Make Coffee, but He Controls 'Starbucks' in Russia*, https://www.nytimes.com/2005/10/12/business/worldbusiness/he-doesnt-make-coffee-but-he-controls-starbucks-in.html (Oct. 12, 2005).

52 *See* Artur Malosiev, *Before bringing the iPhone to Russia, Apple will have to fight for copyright. The Moscow company has already managed to register the trademark,* https://www.iphones.ru/iNotes/822 (Mar. 17, 2015) (stating that "[t]he average price of an assignment of a trademark in the Russian market is $10,000-20,000 . . . . For such an amount, for example, the Russian representative office of Audi bought the rights to the Diablo trademark, under which one of the Lamborghini models is produced").

53 James Grimmelmann, *Internet Law: Cases & Problems*, 384 (12th ed. Semaphore Press 2022).

54 Anne Gilson LaLonde, Gilson on Trademarks § 7A.06 (2010) (quoting 145 Cong. Rec. S9749 (July 29, 1999) (statement of Sen. Hatch)).

'cybersquatter' has acted in 'bad faith,' such as by diverting consumers from the trademark owner's website or registering multiple domain names that are confusingly similar to others' trademarks."[55]

The ACPA creates an *in rem* action to facilitate the recovery of domain names by their rightful owners[56] and provides protection against the bad-faith registration of a domain name[57] made with an intent to profit off of a distinctive mark.[58]

To establish a cybersquatting claim, the trademark owner must show that (1) it had a distinctive or famous mark at the time that the domain name was registered, (2) the defendant registered, trafficked in, or used a domain name that is identical or confusingly similar to plaintiff's mark, and (3) the defendant had a bad faith intent to profit from that mark.[59] The law does not prevent the fair use of trademarks or any use that the First Amendment protects.[60]

The ACPA lists nine non-exclusive factors for courts to consider in determining whether a domain name registrant acted in bad faith.[61] However, courts "need not march through the nine factors

---

55 4 Dunlap-Hanna Pa. Forms § 42.02 (2023).

56 *See* 15 U.S.C. § 1125(d)(2)(A). The ACPA provides that the trademark owner can file an *in rem* action against the domain name in the judicial district where the domain name registrar, domain name registry, or other domain name authority registered or assigned the domain name is located if: 1) the domain name violates any right of the trademark owner; and 2) the court finds that the owner/plaintiff is not able to obtain *in personam* jurisdiction over the person who would have been the defendant or cannot identify a person who would have been a defendant under the ACPA or through due diligence was not able to find a person who would have been a defendant in a civil action by sending or publication of notice related to the alleged violation.

57 Domain name is defined as: "any alphanumeric designation that is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet." 15 U.S.C. § 1127.

58 15 U.S.C. § 1125(d)(1)(A); Attison L. Barnes, III et al., *Fourth Circuit Finds "Re-registration" of a Domain Can be Cybersquatting—A Prudential Clarification to the ACPA*, Wiley Rein, LLP (Jan. 25, 2023), https://www.wiley.law/alert-Fourth-Circuit-Finds-Re-registration-of-a-Domain-Can-be-Cybersquatting-A-Prudential-Clarification-to-the-ACPA.

59 15 U.S.C. § 1125(d)(1)(A); *see also* Mastercard Int'l Inc. v. Trehan, 629 F. Supp. 2d 824, 830 (N.D. Ill. 2009).

60 Gilson, *supra* note 54, § 7A.06.

61 These factors are the following: (I) the trademark or other intellectual property rights of the person, if any, in the domain name; (II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person; (III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services; (IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name; (V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site; (VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the

seriatim because the ACPA itself notes that use of the listed criteria is permissive,"[62] and may also consider "any unique circumstances which do not fit neatly into the specific factors enumerated."[63] Moreover, under the safe harbor provision outlined in 15 U.S.C. § 1125(d)(1)(B)(ii), bad faith intent "shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful."[64] Overall, courts "analyze each case based on its unique circumstances to determine how close a defendant's conduct falls to the ACPA's heartland."[65]

If the trademark owner prevails, the following remedies are available: (i) monetary damages (including maximum statutory damages of $100,000 per act of cybersquatting); (ii) an order canceling the defendant's registration of the offending domain name or transferring it to the trademark owner; and (iii) under "exceptional circumstances"—when the court determines that the defendant willfully or intentionally engaged in cybersquatting—a court may also award attorneys' fees to a winning trademark owner.[66]

To ensure the balance of interests and protect bona fide domain name registrants, the ACPA includes the so-called Reverse Domain Name Hijacking Provision ("RDNH").[67] This provision aims to

---

person's prior conduct indicating a pattern of such conduct; (VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct; (VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and (IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection 15 U.S.C. § 1125(c). *See, e.g.*, Shetel Indus. LLC v. Adin Dental Implant Sys., 493 F. Supp. 3d 64, 130-32 (E.D.N.Y. 2020) (citing 15 U.S.C. § 1125(d)(1)(B)(i)).

62 *Shetel Indus.*, 493 F. Supp. 3d, at 131 (quoting Am. Lecithin Co. v. Rebmann, No. 12-CV-929 (VSB), 2020 WL 4260989, at *8 (S.D.N.Y. July 24, 2020)).

63 *Shetel Indus.*, 493 F. Supp. 3d, at 131 (quoting McAllister Olivarius v. Mermel, 298 F. Supp. 3d 661, 673 (S.D.N.Y. 2018)).

64 Webadviso v. Bank of Am. Corp., 448 F. App'x 95, 98 n.2 (2d Cir. 2011); *see also* Diarama Trading Co. v. J. Walter Thompson U.S.A., Inc., No. 01 Civ. 2950, 2005 U.S. Dist. LEXIS 19496, 2005 WL 2148925, at *13 (S.D.N.Y. Sept. 6, 2005).

65 *Shetel Indus. LLC*, 493 F. Supp. 3d, at 130-32 (quoting New World Sols., Inc. v. NameMedia Inc., 150 F. Supp. 3d 287, 325 (S.D.N.Y. 2015)).

66 15 U.S.C. § 1117(a); § 1117(d); 1125(d); *see also* Hershey Co. v. Anykiss, No. 1:18-CV-00843, 2019 WL 5692738, at *5 (M.D. Pa. Nov. 4, 2019) ("Offending Domain and notice of the Offending Domain's potential for confusion with Plaintiffs' KISSES mark—warrants an award of $100,000, which the Court may exercise its discretion to award.").

67 15 U.S.C. § 1114(2)(D)(v); *see also Reverse Domain Name Hijacking*, ICANNWiki (July 22, 2022), https://icannwiki.org/Reverse_Domain_Name_Hijacking#:~:text=Reverse%20Domain%20Name%20Hijacking%2C%20also,faith%20to%20acquire%20a%20domain (stating that "Reverse Domain Hijacking or Reverse Cybersquatting, involves

protect domain name registrants against unreasonable and unjustified cybersquatting claims. Specifically, "a domain name registrant whose domain name has been suspended, disabled, or transferred" may file a civil action to establish that registering or using the domain name by such registrant is not unlawful.[68] Thus, U.S.-based domain name owners may sue bad faith users of the ACPA for damages up to $100,000 and, in this regard, disincentivize trademark registrants from filing ACPA claims without merit.[69]

As a separate issue, the ACPA addresses the liability of domain name registrars: accredited organizations that register domain names, sell them to the public, and offer hosting, forwarding, and other related services.[70] Section 1114(2)(D)(i) of the ACPA shields registrars from monetary liability from specific core registrar functions in accordance with the ACPA, including if a registrar refuses to register, removes from registration, transfers, temporarily disables, or permanently cancels a domain name (i) in compliance with a court order or (ii) in the course of implementing a registrar's policy aimed at protecting trademark rights.[71] A registrar is also not liable for monetary damages for registering or maintaining a domain name for another party unless the registrar had a bad faith intent to profit from that action.[72] In contrast, registrars can be subject to injunctive relief when they transfer a domain name that is subject to a court action without a court order, refuse to comply with a court order, or fail to deposit certain documents expeditiously in compliance with a court order.[73] However, this injunctive relief is unavailable if the action is pending in a foreign court that is not adjudicating liability under U.S. trademark law.[74]

---

attempting to use trademark protection mechanisms, such as ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) or the Anti-cybersquatting Consumer Protection Act (ACPA), in bad faith to acquire a domain name when the owner has legitimate rights to it").

68 *Id*.

69 15 U.S.C. § 1114(2)(D)(iv)*; see also* Ned T. Himmelrich, Reverse Domain Name Hijacking Can Lead to Liability, Gordon Feinblatt LLC (June 24, 2021), https://www.gfrlaw.com/what-we-do/insights/reverse-domain-name-hijacking-can-lead-liability.

70 15 U.S.C. § 1114(2)(D)(i).

71 15 U.S.C. §§ 1114(2)(D)(i)(I), (ii); *see also* Gilson, *supra* note 54.

72 15 U.S.C. § 1114(2)(D)(iii); *see also* Gilson, *supra* note 54, § 7A.06 n.159 (quoting InvenTel Prods., L.L.C. v. Li, 406 F. Supp. 3d 396 (D.N.J. 2019) ("'[W]ithout a warning that the specific URL being registered would be used for an illicit purpose, [the registrar] did not have a 'bad faith intent to profit' from the automatic registration' of the domain name.")).

73 15 U.S.C. § 1114(2)(D)(i)(II); *see also* Gilson, *supra* note 54.

74 Gilson, *supra* note 54; *see also Zohar Efroni, A Barcelona.Com Analysis: Toward a Better Model for Adjudication of International Domain Name Disputes*, 14 Fordham Intell. Prop. Media & Ent. L.J. 29, 48-51.

Overall, the ACPA provides a comprehensive legal instrument to protect trademark rights against bad-faith registration and cybersquatters' use of domain names. There are significant drawbacks or limitations, however, in that ACPA litigation is typically a lengthy and costly process, and it has limitations with regard to international domain name disputes.

Foreign national anti-cybersquatting laws and approaches vary significantly worldwide, and based on a brief overview of major economic jurisdictions (Brazil,[75] India,[76] Canada,[77] China,[78] the

---

[75] *See* Peter Eduardo Siemsen, Pedro Visconti, *Domain Name Management in Brazil: a Simple Issue for Foreign Entities*, WTR (May 04, 2010), https://www.worldtrademarkreview.com/article/domain-name-management-15; *see also* Brazil – Domain names and trademark infringements, Moeller (Jun. 8, 2018), https://moellerip.com/the-moeller-blog/domain-names-and-trademark-infringements-the-brazilian-experience/.

[76] *See* Sumeet Basu, *Cybersquatting in India - Everything You Need to Know,* Chambers & Partners *(*Aug. 28, 2023), https://chambers.com/articles/cybersquatting-in-india-everything-you-need-to-know; *see also Shivani Singh, Cybersquatting in India* (Dec. 31. 2021), https://blog.ipleaders.in/cybersquatting-in-india/; *see also* Chandler Jesudason, *Landmark cases on domain disputes in India*, iPleaders (Apr. 3, 2021), https://blog.ipleaders.in/landmark-cases-domain-disputes-india/; *see also* Dev Saif Gangjee, *The Polymorphism of Trademark Dilution in India*, 17 Transnat'l L. & Contemp. Probs. 101 (2008).

[77] Jonathan G. Colombo and Catherine Lovrics, *Canadian Domain Name Management: Dot your CA and Protect your IP*, Bereskin & Parr LLP, WTR (2010), https://www.bereskinparr.com/files/file/docs/WTR_JuneJuly_2010_JC_CL.pdf; Christopher Heer, Annette Latoszewska, Michelle Huong, Malcolm Harvey, Stefanie Di Giandomenico, Daryna Kutsyna, *How to Enforce Your Rights in Domain Name Disputes*, Heer Law (Dec. 21, 2022), https://www.heerlaw.com/domain-name-disputes.

[78] *See* Bryan Bachner and Mark Jiang, *Governing Trademarks in Cyberspace: A Comparative Study of the Regulation of Domain Names in China*, 8 Asia Pacific L. Rev 191 (2000); Jyh-An Lee, Domain Name Dispute Resolution in Mainland China and Hong Kong, The Chinese University Of Hong Kong Faculty Of Law Research Paper No. 2020-22 398, 419 (2020).

European Union,[79] Japan,[80] Russia,[81] South Korea,[82] Switzerland,[83] and the United Kingdom[84]), there are only a few examples of comprehensive ACPA-like laws addressing cybersquatting.

There is no unified anticybersquatting law managed on an EU level, and most European countries "extract the bases of anticybersquatting claims from general laws regarding trademarks, unfair completion [sic], passing off, personal and trade name protection."[85] However, a few countries have enacted ACPA-like legislation (e.g., Belgium, Finland, and Denmark).[86] For instance, Finland enacted a Domain Name Act that exhaustively lists the grounds for revocation of a .fi domain name.[87] Similarly, the Belgian

---

79 *See Focus on Cybersquatting: Monitoring and Analysis,* European Union Intellectual Property Office (May, 2021), https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Cybersquatting_Study/2021_Focus_on_Cybersquatting_Monitoring_and_Analysis_Study_FullR_en.pdf; *see also* Ventsislav Pantov, *The Prevention of Cybersquatting in Europe: Diverging Approaches and Prospects for Harmonization* (Sept. 10, 2013) (Master Thesis, Munich Intellectual Property Law Center) [hereinafter *Cybersquatting in Europe*].

80 *See* Brent Yonehara, *Landoftherisingsun.co.jp: A Review of Japan's Protection of Domain Names Against Cybersquatting*, 43 IDEA 207, 212 (2003); *see also* Toki Kawase, *What is the Mechanism of Litigation Regarding Domain Transfer Requests?* (Nov. 22, 2023), https://monolith.law/en/it/domain-trademark-company.

81 *See* Sergey Medvedev, *Resolving Domain Name and Website Disputes in Russia*, Gorodissky (May 21, 2018), https://www.gorodissky.com/publications/articles/resolving-domain-name-and-website-disputes-in-russia/; *see also* Marina Alexandrovna Rozhkova, *Domain Names as Identifiers and Means of Communication ("Доменные имена как идентификаторы и средства коммуникации"),* 3 Economy and Law *("Хозяйство и право")* 55-70 (2015), https://rozhkova.com/pdf/2015-03.pdf.

82 *See* Dong-Hwan Kim, *Registration of Korean Internet domains, and dispute resolution procedures,* Lee International (2011), https://www.inhousecommunity.com/wp-content/uploads/2016/07/v9i3n_jur_SK.pdf; *see also* Yeon-Ho Kim*, The Law and Case Study on the Domain Name Protection (도메인네임의 보호(保護)에 관한 법리(法理) 및 사례연구(事例研究*), 15 Int'l Com. & L. Rev. *(무역상무연구),* 169-209 (2001), https://koreascience.kr/article/JAKO200134406968265.page.

83 *See* Dirk Spacek, *First-step Analysis: Domains & Domain Names in Switzerland,* Lexology (Mar. 26, 2020), https://www.lexology.com/library/detail.aspx?g=0a830b52-af49-468f-8a94-782943ded9ff; *see also* Swiss Federal Institute of Intellectual Property, *Laws*, https://www.ige.ch/en/law-and-policy/international-ip-law/other-organisations/icann/domain-names.

84 *See* David Taylor, *Domains & Domain Names in the United Kingdom,* Lexology (Apr. 11, 2019), https://www.lexology.com/library/detail.aspx?g=20282e5a-0cb9-487e-b6f8-d1e6355a476f; *see also Powers in Relation to UK-Related Domain Name Registries,* DSIT (July 2023), https://assets.publishing.service.gov.uk/media/64b571cd0ea 2cb000d 15e41a/ powers_in_relation_to_uk_related_domain_name_registries_consultation.pdf.

85 *Cybersquatting in Europe,* at III, *supra* note 79 at 32-38 (noting that many European countries have built a solid body of anticybersquatting case law in the realms of trademark law and unfair competition that reflects the application of current laws and approaches (e.g., Germany, France, Norway, Italy, the Czech Republic, Slovakia, Hungary, and Spain)).

86 *Id.*

87 *Id.* at 44; *see also* Domain Name Act (228/2003; amendments up to 397/2009 included) (Fin.), https://www.finlex.fi/en/laki/kaannokset/2003/en20030228_20090397.pdf.

Cybersquatting Act is an anticybersquatting instrument used when .be domain names are involved in a dispute.[88]

Moreover, there is an EU Regulation for.eu (including .ею and .ευ) domain names, according to which companies, individuals, or organizations residing in the EU, Iceland, Liechtenstein, or Norway can register .eu (including .ею and .ευ) domain names.[89] This Regulation includes remedies for transferring or revoking a disputed domain name.[90] Also, in 2019, as part of a collaboration between the EUIPO (the EU Intellectual Property Office) and EURid (the .eu and .ею registry), EUTM (European trademark) applicants and rights holders were allowed to "opt-in to receive alerts as soon as a .eu or .ею domain name identical to their application has been registered."[91] One expert suggests that this EU Framework "could create the scheme for further harmonization of the cybersquatting legislation concerning all ccTLDs in Europe."[92]

Also, European legal scholars propose harmonizing anti-cybersquatting legislation across Europe and, in particular, propose using the experiences of the U.S. and European countries that adopted anticybersquatting legislation to create harmonized ACPA-like legislation.[93] However, the author did not identify any practical steps taken in this regard.

Therefore, for the purposes of this article, the author considers the ACPA as the basis of further analysis of anticybersquatting laws in light of the new challenges presented by Web 3.0.

C. UDRP and Other Alternative Dispute Resolution Procedures for Web 2.0 Domain Names

An alternative (and in some cases the primary) mechanism for rights holders to combat cybersquatting worldwide is to have an alternative dispute resolution ("ADR") procedure adopted for gTLDs and most ccTLDs. Although there are numerous different ADR

---

88 *Cybersquatting in Europe, supra* note 79 at 48-49.

89 Regulation 2019/517 of the European Parliament and of the Council of March 19, 2019, and its accompanying Acts, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0517.

90 *Id.*

91 Jane Seager, *EURid and EUIPO ramp up the fight against cybersquatting*, JDSupra (May 31, 2019), https://www.jdsupra.com/legalnews/eurid-and-euipo-ramp-up-the-fight-98708/; European Commission, *Study on evaluation of practices for combating speculative and abusive domain name registrations,* 5 (July 2020), https://op.europa.eu/en/publication-detail/-/publication/e88d02f9-cbc6-11ea-adf7-01aa75ed71a1/language-en.

92 *Cybersquatting in Europe, supra* note 79, at 23.

93 *Id.; see also* Waddah Alrawashdedh, *In ccTLD, Old Style gTLD and New Style gTLD Systems. Comparative Analysis of the US, EU and International Approaches* (2017), University of Szeged, https://doktori.bibl.u-szeged.hu/id/eprint/4093/1/Waddah_Alrawashdedh_Ertekezes.pdf.

procedures worldwide, including various country-specific ADRs,[94] the leading role is played by the Uniform Domain Name Dispute Resolution Policy ("UDRP") proposed by the World Intellectual Property Organization ("WIPO") and adopted by the ICANN on October 24, 1999.[95]

ICANN's Consensus Policies set forth uniform or coordinated rules of domain name registration and provide a mechanism for rapid, cheap, and reasonable resolution of domain name conflicts by allowing cases to be brought to one of a set of bodies that arbitrate domain name disputes.[96] Domain name registries cannot be accredited by ICANN without agreeing to ICANN's rules, which include provisions that require registries to include specific dispute resolution and UDRP terms in their user agreements such that registrants are required to agree to be subject to UDRP proceedings as a condition to registering their domain name.[97]

The UDRP's jurisdiction covers gTLDs (e.g., .biz, .com, .info, .mobi, .name, .net, .org) and ccTLDs that have adopted the UDRP Policy voluntarily.[98] In this regard, the UDRP applies internationally, and can be used against most foreign cybersquatters who might not be subject to the laws of a plaintiff's home jurisdiction.

UDRP proceedings are conducted by administrative dispute resolution service providers approved by ICANN.[99] WIPO is the largest provider of UDRP services, and it handles UDRP

---

94 *See, e.g.*, *Document Repository* (including EU ADR Rules), EURid, https://eurid.eu/en/other-infomation/document-repository/; *CEPANI Arbitration Rules* (Belgium), CEPANI https://cepani.be/files/publications_documents/documents/rules/en/arbitration/cepani_arbitrage_en---annexes---code-hd.pdf; *.IN Domain Name Dispute Resolution Policy (INDRP)*, https://www.registry.in/domaindisputeresolution; *China ccTLD Dispute Resolution Policy*, CNNIC, https://www.cnnic.com.cn/PublicS/fwzxxgzcfg/201907/t20190726_70774.htm; *.MX Domain name general policies (Mexico)*, https://www.dominios.mx/politicas-generales-de-nombre-de-dominio-mx/.

95 Int'l Corp. for Assigned Names & Numbers, *Uniform Domain Name Dispute Resolution Policy* (Oct. 24, 1999), http://archive.icann.org/en/udrp/udrp-policy-24oct99.htm.

96 Int'l Corp. for Assigned Names & Numbers, *Consensus Policies and Temporary Policies Specification Consensus Policies*, https://www.icann.org/en/system/files/files/proposed-consensus-temporary-policy-07mar13-en.pdf; *see also* Int'l Corp. for Assigned Names & Numbers, *Public Comment Summary Report Registration Data Consensus Policy for gTLDs*, https://itp.cdn.icann.org/en/files/contracted-parties/public-comment-summary-report-registration-data-consensus-policy-gtlds-20-01-2023-en.pdf (last visited Aug. 13, 2024).

97 *Registrar Accreditation Agreement*, Int'l Corp. for Assigned Names & Numbers (Aug. 2, 2012), https://www.icann.org/resources/pages/ra-agreement-2009-05-21-en.

98 ccTLDs adopting the UDRP include .ag, .ai, .as, .bm, .bs, .bz, .cc, .cd, .co, .cy, .dj, .ec, .fj, .fm, .gd, .gt, .ki, .la, .lc, .md, .me, .mw, .nr, .nu, .pa, .pk, .pn, .pr, .pw, .ro, .sa, .sc, .sl, .sn, .so, .tj, .tt, .tv, .ug, .ve, .vg, and .ws. *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*, WIPO, https://www.wipo.int/amc/en/domains/guide/ (last visited Aug. 16, 2024) [hereinafter *WIPO Guide*].

99 *Id.*; *see also, e.g.*, Sallen v. Corinthians Licenciamentos LTDA, 273 F.3d 14, 21 (1st Cir. 2001).

proceedings for gTLDs and over 80 ccTLDs.[100] As stated on the WIPO website, "[i]ts expertise to administer domain name disputes stems from its involvement in the international process conducted by WIPO at the request of its member States which led to the UDRP Policy and Rules."[101]

The WIPO Center decides many cybersquatting disputes. For example, in 2022, trademark owners filed a record (in comparison with previous years) 5,764 cases with the WIPO Center under the UDRP.[102] In 2023, this amount was even higher—with 6,192 cases filed.[103] WIPO UDRP cases in 2023 involved parties from 185 countries and involved more than 120,000 Internet domain names.[104]

As for the substance of the UDRP complaints, similar to the ACPA, under the UDRP, the trademark owner must prove that (i) the allegedly infringing domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; (ii) the alleged infringer has no rights or legitimate interests in the domain name; (iii) and the allegedly infringing domain name has been registered and is being used in bad faith.[105]

Moreover, the UDRP procedures include certain ACPA-like mechanisms to ensure the balance of interests and prevent "the harassment of domain name holders acting in good faith by trademark owners."[106] Rule 15(e) of the UDRP states that "if after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding."[107] In this regard, the UDRP procedures

---

100 Ivett Paulovics, Andrzej Duda, Maciej Korczynski, *Study on Domain Name System (DNS) Abuse,* 77-78, European Commission (July 2022), https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1; *see also WIPO Caseload Summary* (2023), WIPO, https://www.wipo.int/amc/en/center/caseload.html?utm_source=WIPO+Newsletters&utm_campaign=e67a58af31-DIS_ADR_EN_190123&utm_medium=email&utm_term=0_bcb3de19b4-e67a58af31-256979998&ct=t(DIS_ADR_EN_190123) [hereinafter *WIPO Caseload Summary*].

101 *WIPO Guide, supra* note 98.

102 *WIPO Caseload Summary, supra* note 100*; see also Domain Name Dispute Resolution Service for Country Code Top Level Domains* (ccTLDs), WIPO, https://www.wipo.int/amc/en/domains/cctld/ (last visited Aug. 13, 2024).

103 *WIPO Caseload Summary, supra* note 100.

104 *Id.*

105 Terese L. Arenth, *supra* note 28.

106 WIPO, *Final Report of the WIPO Internet Domain Name Process* (Apr. 30, 1999), https://www.wipo.int/amc/en/processes/process1/report/finalreport.html.

107 Int'l Corp. for Assigned Names & Numbers, *Rules for Uniform Domain Name Dispute Resolution Policy*, https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en (last visited Aug. 13, 2024).

include similar protections against unfair actions by trademark holders as those in the ACPA.

However, unlike the ACPA, the UDRP does not require that the trademark at issue be distinctive or famous at the time of the domain name registration.[108] Therefore, even holders of after-acquired trademark rights may seek relief under the UDRP.[109] Moreover, the application of the UDRP by the WIPO panel heavily relies on specific rules and tests in deciding domain name disputes that might be different from the ACPA's interpretation by federal courts.[110] For example, UDRP proceedings are not based on the comprehensive evidentiary rules and guidelines available to ACPA litigants in federal courts.[111]

Also, UDRP proceedings at the WIPO Center can cover infringing activities that might be outside the scope of ACPA. This includes certain common law trademarks, personal names, and even exceptional geographical indications that are not registered as trademarks, but which can be enforced in a UDRP action "if the complainant is able to show that it has rights in the term sufficient to demonstrate consumer recognition of the mark in relation to the complainant's goods or services."[112]

Remedies available to trademark owners under the UDRP are also more limited than those available under the ACPA, namely, these remedies are limited to the transfer or cancellation of the infringing domain name by the domain name registrar; no monetary damages are available.[113] Nor can a UDRP panel award attorney's fees.[114] Moreover, national courts applying national laws could trump (by reviewing a case *de novo*) UDRP rulings, and, therefore, a UDRP decision does not prevent a court from applying domestic law in trademark domain name disputes.[115]

---

108 Kurtzman, *supra,* note 29.

109 *Id.*

110 *WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Jurisprudential Overview 3.0"),* (2017), https://www.wipo.int/amc/en/domains/search/overview3.0/.

111 *See, e.g.,* Connie L. Ellerbach, *UDRP Versus ACPA: Choosing the Right Tool to Challenge Cybersquatting*, Fenwick & West (Sept. 29, 2003), https://assets.fenwick.com/legacy/FenwickDocuments/UDRP_Versus_ACPA.pdf.

112 *Id.*

113 *WIPO Guide*, *supra* note 98.

114 *Id.*

115 *Final Report of the WIPO Internet Domain Name Process, supra* note 106; *see also* Frederick W. Mostert and Martin B. Schwimmer, *Notice and Takedown For Trademarks,* Vol. 101 No. 1 TMR 268 (Jan.-Feb. 2011) (stating that "UDRP cases have no influence on civil courts and thus do not abrogate the civil rights of the parties" and quoting Barcelona.com v. Excelentisimo Ayuntamiento de Barcelona, 189 F. Supp. 3d 367 (E.D. Va. 2002), *rev'd*, 330 F.3d 617 (4th Cir. 2003)); *see also* Laurence R. Helfer, *Whither the UDRP: Autonomous, Americanized or Cosmopolitan?* 12 Cardozo Int'l & Comp. L. Rev. 493, 494 (2004) (symposium on ICANN, ccTLD, and the Legacy Root),

For gTLDs and a substantial number of ccTLDs registered through an ICANN-accredited registrar, the domain name registration agreement will include a requirement that the domain name owner agree to be subject to the UDRP.[116] In contrast, bringing a civil action for cybersquatting typically requires the plaintiff to establish that the court has jurisdiction. In any case, if either party to the UDRP proceeding disagrees with the decision, they can still file a civil action in court.[117] Moreover, parallel proceedings might be possible in some instances.[118] Overall, while UDRP proceedings are less costly and faster than alternative options, and jurisdiction is usually a simpler question, litigation in courts gives access to a more detailed examination of facts and discovery procedures and allows a plaintiff to receive monetary damages.[119] Potential plaintiffs need to consider the appropriate forum carefully, and if the dispute involves a defendant located where jurisdiction may be difficult to establish, or if the primary goal is to stop the infringement as soon as possible, a UDPR proceeding may be preferred to civil litigation in national courts.

Additionally, for some ICANN-coordinated domain names, primarily gTLDs, there are additional legal procedures aimed at assisting trademark owners from all over the world in protecting their rights. For example, Uniform Rapid Suspension ("URS") allows trademark owners to file a complaint and suspend a registered domain name in clearly established infringement cases.[120] The burden of proof is clear and convincing evidence.[121] Certified examiners determine whether to suspend or not to suspend the domain name.[122] If the examiner's determination is in favor of the complainant, the domain name is suspended and will

---

https://scholarship.law.duke.edu/faculty_scholarship/2009/.

116 *Final Report of the WIPO Internet Domain Name Process, supra* note 106.

117 *Id.; see also* Sallen v. Corinthians Licenciamentos LTDA, 273 F.3d 14, 26 (1st Cir. 2001) (the UDRP clearly contemplates judicial intervention and, in fact, that the judicial outcome will override the UDRP one (citing UDRP 4(k))); *see also* Pocketbook Int'l SA v. Domain Admin/SiteTools, Inc., No. CV 20-8708-DMG (PDX), 2021 WL 1422784, at *4 (C.D. Cal. Apr. 13, 2021) ("The Court agrees with the First, Second, and Fourth Circuits that the UDRP does not contemplate that its alternative dispute resolution panels shall make final decisions that have preclusive effect on contemporaneous or subsequent civil actions . . . [c]itation to an unpublished district court case giving collateral estoppel effect to the findings of a UDRP panel is unpersuasive.") (internal citations omitted).

118 *See, e.g.*, Parisi v. Netlearning, Inc., 139 F. Supp. 2d 745, 751 (E.D. Va. 2001) ("[T]he UDRP contemplates parallel litigation. Nothing in the UDRP restrains either party from filing suit before, after, or during the administrative proceedings.).

119 *Id.*; *see also* John Hartje, *Resolving Internet Domain Disputes*, Intellectual Property Today (Aug. 15, 2000) at 38.

120 Int'l Corp. for Assigned Names & Numbers, *Uniform Rapid Suspension (URS)*, https://www.icann.org/resources/pages/urs-2014-01-09-en (last visited Aug. 13, 2024).

121 *Id.*

122 *Id.*

not be able to be transferred, deleted, or modified for the life of the registration.[123]

Moreover, Post-Delegation Dispute Resolution Procedures ("PDDRP") provide rights holders with an alternative dispute resolution mechanism to resolve claims that a registry operator intentionally and systematically infringes trademarks in its TLDs, either by itself or by aiding third parties.[124] There are three kinds of PDDRPs: 1) Trademark Post-Delegation Dispute Resolution Procedure ("Trademark PDDRP"); 2) Registry Restriction Dispute Resolution Procedure ("RRDRP"); and 3) Public Interest Commitments Dispute Resolution Procedure ("PICDRP").[125] The Trademark PDDRP generally addresses alleged trademark infringements on a new gTLD's first or second level.[126] Such dispute resolution procedures are handled by providers external to ICANN and are binding on the parties.[127] If the parties do not comply with the determination, the provider may take further action, such as ordering the parties to pay damages or to transfer the infringing domain name to the complainant.[128]

Finally, WHOIS, a global database of all registered domain names, is a helpful transparency tool for trademark holders.[129] When somebody registers a domain name, the registrant must provide the registrar with contact information (e.g., name, address, phone number).[130] Although this information is usually masked due to privacy considerations and GDPR requirements, trademark holders can use WHOIS to find information about the registrar and unmask the identity of the registrant through the discovery process when legal proceedings are initiated.[131] Also, for the new gTLD registries and registrars, ICANN has a database of validated and registered trademarks to assist trademark holders in preventing infringing behavior in the Domain Name System, The Trademark

---

123 *Id.*

124 Int'l Corp. for Assigned Names & Numbers, *Understanding Post-Delegation Dispute Resolution Procedures*, https://newgtlds.icann.org/en/program-status/pddrp (last visited Aug. 13, 2024); *see also Trademark Post-Delegation Dispute Resolution Procedure*, Int'l Corp. for Assigned Names & Numbers, https://icannportal.force.com/compliance/s/trademark-post-delegation-dispute (last visited Aug. 13, 2024).

125 *Understanding Post-Delegation*, *supra* note 124.

126 *Id.*

127 *Id.*

128 *Id.*

129 *Registration data lookup tool*, Int'l Corp. for Assigned Names & Numbers, https://lookup.icann.org/en (last visited Aug. 13, 2024).

130 *About WHOIS*, Int'l Corp. for Assigned Names & Numbers, https://www.icann.org/resources/pages/what-2013-03-22-en#:~:text=Whois%20is%20an%20Internet%20protocol,name%20(or%20IP%20address) (last visited Aug. 13, 2024).

131 *Id.*

Clearinghouse.[132] The Trademark Clearinghouse authenticates information from rights holders and provides right holders with notifications when a domain name matching the trademark is registered.[133]

Overall, the current ACPA-UDRP framework and other ICANN-coordinated tools provide a working, although imperfect, framework for trademark owners to protect their intellectual property rights and fight the bad faith registration of ICANN-coordinated domain names.

PART II. GLOBAL CHALLENGES FOR TRADEMARK PROTECTION IN WEB 3.0: BLOCKCHAIN DOMAIN NAMES AND CYBERSQUATTING

A. The Rise of the Blockchain Domain Name System as the Most Promising Alternative Domain Name System

Alternative root servers and alternative domain name systems have existed since the late 1990s.[134] Alternative root servers are "either systems not based on the DNS protocol at all or systems based on the DNS protocol but whose contents deviate from the IANA promulgated authoritative root zone file."[135] Alternative domain name systems might be run for different reasons, including for idealistic, ideological, security-related, and profit-related reasons.[136] Historical examples of alternative domain name systems include such projects as:

- AlterNIC, a domain name registry created in the late 90s that relied on an alternative DNS root and existed prior to the creation of ICANN;[137]
- Open Root Server Network, a network of root servers in Europe that operated from February 2002 to December 2008;[138]

---

132 *Understanding the Trademark Clearinghouse*, Int'l Corp. for Assigned Names & Numbers, https://newgtlds.icann.org/en/about/trademark-clearinghouse (last visited Aug. 13, 2024).

133 *Id.*

134 *Alternative Roots*, ICANNWiki (July 22, 2022), https://icannwiki.org/Alternative_Roots.

135 *Id. See also Challenges with Alternative Name Systems*, *supra* note 23 ("There are broadly two kinds of alternative naming systems: (i) Those based on the DNS protocol but using an alternative root; Those not based on the DNS protocol.").

136 *Alternative Roots*, *supra* note 134.

137 *Id.*

138 *Open Root Server Network*, ICANNWiki (Aug. 25, 2022), https://icannwiki.org/Open_Root_Server_Network#:~:text=The%20Open%20Root%20Server%20Network,the%20network%20coordinated%20by%20ICANN.

- RealNames, a DNS offered by Microsoft on its Internet Explorer browser address bar before 2002;[139]
- The Handle System, a part of the Digital Object Architecture;[140]
- The Onion system is used by the TOR project;[141]
- The Russian National Domain Name System, an alternative DNS root project started in 2019 by the Russian government agency;[142] and
- The Yeti DNS Project, sponsored by a Chinese state agency, is an alternative root server dedicated to IPv6 and aimed at experimenting with different new DNS-related technologies.[143]

In addition to these projects, in the 2010s, numerous blockchain-based projects emerged and led to the creation of blockchain-based alternative domain name systems. For example, Namecoin is "one of the earliest attempts at a blockchain-based naming system."[144] Namecoin is an experimental fork of Bitcoin that uses the .bit TLD and is the equivalent of a second-level domain name.[145] Currently, several blockchain-based naming systems are in operation, some of which are equivalent to second-level domains, and some are equivalent to TLDs.[146] As noticed in a study by Oxford Informational Labs researchers, "[b]lockchain domain names are a new alt-root with a wide literature gap that requires critical attention."[147] Like other alternative domain name systems, blockchain-based systems do not use ICANN-controlled DNS servers to connect an IP address to the Internet.[148] However, blockchain-based systems uniquely link

---

139 *RealNames*, Wikipedia (Oct. 5, 2018), https://en.wikipedia.org/wiki/RealNames.

140 *Digital Object Architecture and the Handle System*, ICANN (Oct. 14, 2019), https://www.icann.org/en/system/files/files/octo-002-14oct19-en.pdf.

141 Jacob Appelbaum, *The ".onion" Special-Use Domain Name*, Internet Engineering Task Force (IETF), https://datatracker.ietf.org/doc/html/rfc7686; *see also Overview of the Digital Object Architecture (DOA)*, Internet Society (Oct. 26, 2022), https://www.Internetsociety.org/resources/doc/2016/overview-of-the-digital-object-architecture-doa/.

142 Naveen Goud, Russia creates its own Domain Name System Internet, Cybersecurity Insiders https://www.cybersecurity-insiders.com/russia-creates-its-own-domain-name-system-Internet/ (last visited Aug. 13, 2024).

143 *Yeti DNS Project Phase-2*, Yeti DNS (2019), https://yeti-dns.org/ (last visited Aug. 13, 2024).

144 *Challenges with Alternative Name Systems*, *supra* note 23.

145 *Id.*

146 *Id.*

147 *Web3 disruption*, *supra* note 10, at 143.

148 *Challenges with Alternative Name Systems*, *supra* note 23.

an IP address via decentralized P2P networks, without a central storage point.[149]

Indeed, the milestone in developing alternative domain names, particularly BDNs, was the rise of blockchain technologies and the market for non-fungible tokens ("NFTs") in the last several years. NFTs are digital certificates that authenticate the ownership of assets.[150] NFTs are created or "minted" using a digital blockchain ledger or other similar "web3" technology.[151] Devin Finzer describes NFTs and points out that: "Non-fungible tokens (NFTs) are 'unique, digital items with blockchain-managed ownership.'"[152] What makes NFTs unique is their "non-fungibility" (i.e., there is only one version of the particular line of code comprising any single NFT so that it is not fungible or exchangeable with any other token on a like-for-like basis).[153] Non-fungibility distinguishes NFTs from other blockchain-based tokens such as cryptocurrencies, which are interchangeable.[154] NFTs are minted (i.e., created via immutable (unalterable) entry on the blockchain) and transferred from one owner to another via smart contracts (i.e., "self-executing contracts or lines of computer code on a blockchain").[155]

According to Eric Anziani, COO of Crypto.com, "NFTs really started initially with the digital art side. But it's going to be a lot more powerful. . . . It will be the tool that represents any digital type of assets in virtual worlds going forward. So, the applications are

---

149 *Id.; see also* Chen Wang, Jin Zhao: Network approaches in blockchain-based systems: Applications, challenges, and future directions. 212 Comput. Commun. 141-150 (2023), https://www.sciencedirect.com/science/article/abs/pii/S0140366423003298 ("Most current decentralized P2P networks utilize Internet Protocol version 6 (IPv6) in Internet of Things (IoT) environments instead of IPv4, allowing each end user to have a unique IP address for network identification purposes. Blockchain-based systems are built atop P2P networks, and without a central storage point, it becomes difficult for information to be hacked").

150 Gilson, *supra* note 54, § 7A.18 (noting that "[t]hese assets include digital 2D or 3D art, music, an in-game item, videos, sports highlights, social media posts, GIFs, concert clips, admission tickets, inclusion in an online community, and many others. NFTs are unique units of data that cannot be replaced, replicated, or destroyed.").

151 *See, e.g.*, *Kevin* Roose, "*What is web3?,*" N.Y. Times (March 18, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/web3-definition-internet.html; *see also* Thomas Stackpole, "*What is Web3?*," Harv. Bus. Rev. (Sept. 25, 2022), https://hbr.org/2022/05/what-is-web3.

152 Devin Finzer, *The Non-Fungible Token Bible: Everything you need to know about NFTs*, OpenSea (Jan. 10, 2020), https://blog-v3.opensea.io/articles/non-fungible-tokens.

153 *See, e.g., Non-Fungible Tokens (NFTs*), Congressional Research Service (July 20, 2022), https://crsreports.congress.gov/product/pdf/R/R47189; Discover NFTs: Your Ultimate Guide to Non-Fungible Tokens (May 21, 2024), https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-nft#:~:text=For%20example%2C%20one%20Bitcoin%20is,no%20two%20NFTs%20are%20identical.

154 *See Non-Fungible Tokens (NFTs*), *supra* note 153.

155 *Id.*

tremendous."[156] NFTs, powered by blockchain, found a new application in domain name registration and specifically enabled the development of the so-called Web 3.0 and BDNs.

BDNs are NFTs that can be bought, sold, or transferred.[157] BDNs link a domain name to a specific smart contract address on a blockchain, and in most cases, the owner of the address linked to the BDN may also point the BDN to a website on a peer-to-peer Internet system or the traditional Internet.[158] For example, the Ethereum Name Service ("ENS") creates an Ethereum NFT (ERC-721)[159] that consists of a name along with an ".eth" extension.[160] The ENS combines two smart contracts on the Ethereum blockchain, allowing domain name registration and lookup services.[161] ENS offers human-readable domains (i.e., in characters, e.g., such as "example.com" rather than IP address).[162] Moreover, it is now possible to use ENS domains as traditional Web 2.0 domain names for hosting a website, and some new BDNs (e.g., .box domains introduced in April 2024) are even compatible with standard browsers and can operate as Web 2.0 domains.[163]

---

156 *NFTs: The metaverse economy*, Fin. Times, https://www.ft.com/partnercontent/crypto-com/nfts-the-metaverse-economy.html (quoting Eric Anziani, COO of Crypto.com) (last visited Aug. 13, 2024).

157 John Melcher, *The rise of blockchain domain NFTs*, Exodus (Mar. 14, 2022), https://www.exodus.com/news/blockchain-domain-nfts/ [https://perma.cc/8U7X-HESQ].

158 Andrea Calvaruso et. al., *Unauthorized Blockchain Domain Names: What's a Brand to Do?*, JDSupra (Mar. 8, 2022), https://www.jdsupra.com/legalnews/unauthorized-blockchain-domain-names-5919874/.

159 Corwin Smith, *ERC-721 Non-Fungible Token Standard*, Ethereum (Apr. 7, 2023), https://ethereum.org/en/developers/docs/standards/tokens/erc-721/.

160 *See, e.g.*, Andrew Carr, *.ETH Domains with Ethereum Name Service (ENS)?*, Atomic Wallet (Apr. 2, 2024), https://atomicwallet.io/academy/articles/eth-domains [hereinafter *.ETH Domains*].

161 *See, e.g.*, Zoltan Vardai, *What is ENS (Ethereum Name Service) and how does it work?*, Forkast (Dec. 8, 2021), https://forkast.news/what-is-ens-ethereum-name-service-how-does-it-work/#:~:text=ENS%20is%20built%20on%20two%20Ethereum%20smart%20contracts.,caching%20time%20for%20all%20records%20under%20the%20domain [hereinafter *What is ENS*]; *see also* Ayushi Abrol, *What Is ENS (Ethereum Name Service) And How Does It Work?,* Blockchain Council (Nov. 14, 2022), https://www.blockchain-council.org/ethereum/ethereum-name-service/ ("The first smart contract holds three important pieces of information: (i) First is the details of the domain like the owner of the domain; (ii) The second is the resolver for the domain; (iii) The third is caching time for all the records under the specific domain. The second contract that is a part of ENS is Resolver: (i) The resolver is the smart contract that converts the machine-readable address to human-readable and vice versa; (ii) It matches the domain name to an individual, website, or address.").

162 *What is ENS*, *supra* note 161; *see also .ETH Domains*, *supra* note 160 ("For example, instead of sending Ethereum to an address like "0x4cbe . . .", you could send it to 'yourname.eth'").

163 *.ETH Domains*, *supra* note 160 ("Decentralized websites can be hosted via IPFS hashes, or the TOR-address via the TOR Browser. It is difficult or impossible to censure IPFS or TOR Web-addresses, and these difficult to read (hashed) IPFS or TOR addresses cab be linked to, and made human-readable, via Web3 ENS Names. These Web3 ENS addresses

BDNs are managed by decentralized domain registrars and can be owned and controlled by individuals or organizations, rather than by centralized entities such as ICANN and accredited registrars.[164] Various BDN services exist, including Handshake (Namecheap), Unstoppable Domains, Decentraweb, and Ethereum Name Service (ENS).[165] Some of these services use rental and expiration systems similar to typical domain name registrars (e.g., ENS), while some other BDN services operate via purchases and do not require renewals to maintain and use BDNs (e.g., Unstoppable Domains).[166] Different BDN extensions and TLDs exist, such as .nft, .crypto, and .blockchain. Also, some companies allow users to create and own personalized TLDs and second-level domains.[167]

As noted by Brad Kam, co-founder of Unstoppable Domain, "for the almost 30 years of history of DNS, there's really been one DNS system the entire internet has been using," and "this is really the first time we're seeing browsers have embraced an alternative system."[168] As of December 2023, more than 12 million BDNs had been registered in Handshake.[169] Also, as of March 2024, there are some 2,070,016 active ENS.[170] And, as of March 2024, the number of purchased or minted Unstoppable BDNs exceeds 3.4 million.[171] Many experts predict an upcoming boom of BDN registrations, especially considering the claims of BDN providers that users will

---

are still new. There are semi-decentralized services that allow you to resolve ENS-Websites, by adding ".limo" or ".link" to the end of the ENS-Website-Name"); *see also Web3 Innovation, supra* note 6; *see also Web2+Web3 In One Powerful Domain*, My.box, https://www.my.box/ [hereinafter *Web2+Web3*] (last visited Aug. 16, 2024) (stating that ".box domains are uniquely crafted to be compatible with both Web2 and Web3 infrastructures, enabling them to interact with traditional web services while retaining decentralized benefits.").

164 *Id.*

165 Ivanontech, *How to Build a Web3 Website*, Moralis Academy (May 9, 2022), https://academy.moralis.io/blockchain-guides/how-to-build-a-web3-website.

166 *See, e.g.,* Unstoppable Domains, https://unstoppabledomains.com/ (last visited Aug. 13, 2024).

167 *See, e.g.,* Freename, https://freename.io/ ("Web3 Domain names — you can build your own Web3 domain ecosystem and become a registrar yourself"); *see also* Decentraweb, *Decentraweb—Top & Sub-level Domains V3—Collection | OpenSea,* OpenSea https://opensea.io/assets/ethereum/0x3eaf3d0e21f452adf632744b5608e6c02e88827a/20146914403306250624663396699041985666657175358672255074736328635174807923422 ("Anyone can permissionessly [sic] create their own top level domain (TLD) and own it permanently on the Ethereum blockchain.").

168 Benjamin Powers, *Brave Integrates. Crypto Blockchain Domains, Expanding Access to Web 3.0*, CoinDesk (May 13, 2021), https://www.coindesk.com/tech/2021/05/13/brave-integrates-crypto-blockchain-domains-expanding-access-to-web-30/?outputType=amp.

169 *Handshake Statistics*, Namebase, https://www.namebase.io/stats/#usage (last visited Aug. 13, 2024).

170 Makoto, *@makoto / ENS*, Dune Community Discord, https://dune.xyz/makoto/ens (last visited Aug. 13, 2024).

171 Unstoppable domains, *supra* note 166.

technologically need only an Internet connection, regardless of the user's chosen web browser, to register and use BDNs, including recent (as for May 2024) initiatives related to Web 2.0 and Web 3.0 interoperability.[172]

Currently, BDNs require customers to use specific Web 3.0 technological solutions (rather than standard Web 2.0 browsers and networks), and are primarily used for crypto-payments (for instance, .crypto domains work inside fifty different crypto wallets and exchanges).[173] However, current BDNs can also point to content hosted on a blockchain, like a website.[174] For example, the Brad.crypto domain hosts an NFT art gallery owned by Brad Kam, co-founder of Unstoppable Domain.[175] Numerous other examples illustrate BDNs that host websites (e.g., thebasics.crypto, a website with live news about the cryptocurrency market, and dtube, a crypto community-powered video sharing platform).[176]

BDNs have certain advantages over ICANN-coordinated domain names, which include more flexibility, less censorship or control of any single entity, and the possibility for customers to permanently own and control particular BDNs, including further resale on open markets such as OpenSea.[177]

Despite BDN providers usually denying competition or any direct naming collisions with ICANN-coordinated domain names,[178]

---

172 Joel Khalili, *You can now access blockchain domains using any web browser*, TechRadar (Feb. 16, 2021) https://www.techradar.com/news/youll-soon-be-able-to-access-blockchain-domains-using-any-web-browser ("Blockchain domain registry Unstoppable Domains has unveiled a new service that expands access to decentralized websites to anyone with an Internet connection"); *see also D3. The First Interoperable Namespace Network*, https://d3.inc/ ("In partnership with leading Web3 ecosystems, D3 intends to apply for and acquire new Top Level Domains (TLDs) during ICANN's upcoming application window to give users secure identities with enhanced utility, security, Web3-compatability, and universal access on critical Internet infrastructure."); *see also Web3 Domain Industry Growth: A Look Into The Future*, Freename.io, https://freename.io/web3-domain-industry-growth/ (". . . we can expect the market for Web3 domains to grow even more. Analysts forecast that the Web3 domain market could reach a valuation of $81.5 billion by 2030, up from $3.2 billion in 2021.").

173 Benjamin Powers, *supra* note 168; *see also Support Unstoppable Domains in Your Web Browser*, Unstoppable domains, https://docs.unstoppabledomains.com/use-cases/support-ud-browser/ (last visited Aug. 13, 2024); *see also Challenges with Alternative Name Systems*, *supra* note 23 at 8-10 (discussing "[a] number of bridging (or transition) techniques exist to enable early adopters to reach names using alternative naming systems.").

174 Benjamin Powers, *supra* note 168.

175 *Id.*

176 *Id.*

177 *The Future of Web3 Domains and Opportunities for Brands*, GrowthChain (Jan. 21, 2023), https://www.growthchain.io/blog/web3-domains; *see also Web3 disruption*, *supra* note 10.

178 *See, e.g.*, *Web3 Domain Alliance Launches to Protect Users' Digital Identities*, Newsfile Corp. (Nov. 3, 2022), https://www.newsfilecorp.com/release/142928/Web3-Domain-Alliance-Launches-To-Protect-Users-Digital-Identities ("the Web3 Domain Alliance aims to proactively engage in discussions with ICANN to increase ICANN's awareness

certain actors indicate a perspective for BDNs to supplant the current DNS.[179] In this regard, interestingly, Namecheap, an ICANN-accredited registrar,[180] advertises BDNs for sale through the use of a "decentralized, permissionless naming protocol" from a third party, Handshake,[181] and describes BDNs as a "new approach to domain name ownership," which can be used for "bypassing the traditional organizations and registries that call the shots online."[182] Moreover, at the end of 2023, Unstoppable Domains expanded its offerings by incorporating traditional ".com" addresses.[183] Experts have claimed that this integration is groundbreaking since "[t]his move marks the first instance of merging conventional Web2 domains with the evolving Web3 domain space."[184] This integration "aims to seamlessly connect the existing web infrastructure with the new" and "eliminates the need for users to navigate different systems, reducing friction and enhancing overall efficiency in managing financial resources."[185]

Although ICANN has not yet taken a position on BDNs, it has previously expressed some concerns about them.[186] At the same time, recent initiatives suggest that some BDN providers might be interested in partnering with ICANN and developing BDNs interoperable with Web 2.0 domains (i.e., make BDNs that could

---

and recognition of W3TLDs"); *see also* Tom Barrett, *Will Web3 Make ICANN Obsolete?*, Forbes (July 13, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/07/13/will-web3-make-icann-obsolete/ ("ICANN is not going to go away. But I do not believe it is going to become the regulator for Web3, either."); *see also* Brantly Millegan, *Linking DNS with blockchain-based ENS records*, ICANN (Jun. 24, 2019), https://ccnso.icann.org/sites/default/files/field-attached/presentation-dns-blockchain-ens-24jun19-en.pdf (discussing collaboration and integration initiatives between Ethereum and ICANN).

179 *See, e.g.*, Toshendra Kumar Sharma, *Could Blockchain Replace DNS?*, Blockchain Council (March 24, 2018), https://www.blockchain-council.org/blockchain/blockchain-replace-dns/; *see also* Roger LaLonde et. al., *Resolution of the American Bar Association Section of Intellectual Property Law, Committee No. 206, Support for Legislation that Amends or Supplements Existing Intellectual Property Law to Address Infringing Uses of Blockchain Domain Names and Similar Web3 Naming Applications*, ABA Trademarks and the Internet Committee (Apr. 12, 2023) (unpublished resolution; approved by ABA Section of Intellectual Property Law) (on file with author).

180 *Handshake Domains,* NameCheap, https://www.namecheap.com/support/knowledgebase/article.aspx/10484/2278/namecheap-handshake-tlds/ (last visited Aug. 13, 2024).

181 *Decentralized naming and certificate authority*, HandShake, https://handshake.org/ (last visited Aug. 13, 2024).

182 *Handshake Domains, supra* note 180.

183 Anthony Clarke, *A closer look at Unstoppable Domains' .com integration*, Cointelegraph (Dec. 18, 2023), https://cointelegraph.com/news/unstoppable-domains-com-integration-closer-look.

184 *Id.*

185 *Id.*

186 *See* Alain Durand, *Buyer Beware: Not All Names Are Created Equal*, ICANN (Nov. 24, 2021), https://www.icann.org/en/blogs/details/buyer-beware-not-all-names-are-created-equal-24-11-2021-en ("discussing potential collision between DNS and BDNs and numerous other risks associated with BDNs.")

have an IP address and Web2 domain name associated with it, and, in this way, BDN would "resolve on Web2, the Internet as we know it, while simultaneously . . . resolv[ing] across the Ethereum, Bitcoin, Polygon, etc. blockchains"[187]) and particularly to apply for new gTLDs that ICANN plans to implement by the second quarter of 2026.[188] However, it is unclear whether ICANN would be open to this partnership.

For now, due to the anonymous and decentralized nature of BDNs, the lack of uniform technical connection to the ICANN-coordinated domain name system, particular legislation, or even recognized industry rules, BDNs reveal serious risks of violations of third parties' rights, especially trademark rights.[189]

B. Cryptosquatting: Shortcomings of the Trademark Protection Framework in Web 3.0

1. Practical Barriers for Trademark Protection in Web 3.0

Web 3.0 currently allows users to register BDNs containing designations identical or similar to registered trademarks, including various well-known trademarks. For example, as of October 2023, Unstoppable Domains enables users to buy such BDNs as celine.nft (available for $600), chanelofficial.x (available for $40); hermesofficial.nft (available for $20); harvardlaw.blockchain (available for $10); and cardozolaw.go (available for $20).[190] Many BDNs that contain well-known trademarks are already taken or are available for sale (e.g., "lvmh" (all extensions); "google" (all extensions); diorofficial.nft; harvardlaw.crypto; and harrypotter.crypto).[191] As with traditional domain name registrations, it is difficult, if not impossible, to determine whether these BDN registrations are owned by the right holders or by unrelated third parties because of the anonymity of the domain owners and the implementation of privacy shielding systems that would not allow to see the registrants. Moreover, as for

---

187 *Web3 Innovation, supra* note 6.

188 *Id.*; *see also* Cointelegraph, *Unstoppable Domains to apply for '.blockchain' domain registration.*, CoinMarketCap (June 6, 2024), https://coinmarketcap.com/community/articles/6661de0a8da01a19fba0f286/.

189 Giovanna H. Fessenden, *Web3 Blockchain Domain Names: A New Frontier for Trademark Protection*, Hamilton, Brook, Smith & Reynolds, P.C. (Apr. 15, 2022), https://www.hbsr.com/news-insights/web3-blockchain-domain-nfts-a-new-frontier-for-trademark-protection; *see also* Kristian Elftorp, Knud Wallberg, Niclas Jonsson, *How Blockchain domain names could become the next online property boom*, Managing IP (Feb. 14, 2023), https://www.managingip.com/article/2ba3e9pcxgva00q2d1af4/sponsored-content/how-blockchain-domain-names-could-become-the-next-online-property-boom.

190 Unstoppable Domains, *supra* note 166.

191 *Id.*

the BDNs, most providers do not have comprehensive rules or policies like the ICANN Registration Data Policy outlining the requirements and processes underlying the processing of registrant's personal information, including disclosure requests; therefore, the unmasking process with respect to BDNs' registrants might be more unpredictable and challenging.[192]

Also, many BDNs are available via online markets such as OpenSea, Rarible, Mintable, Kraken NFT Marketplace, Binance NFT Marketplace, or the Coinbase NFT Marketplace. For example, in July 2022, the domain "amazon.eth" was offered for public sale on OpenSea, and an offer for $1 million was received from an anonymous wallet address on OpenSea.[193] Although the offer to buy the ENS domain went unanswered, no transaction took place, and the offer to sell this domain name expired,[194] this example illustrates the value of BDNs identical to famous trademarks and the potential for abuse (especially given the lack of a comprehensive enforcement mechanism). Moreover, as of April 2023, searching "amazon" on OpenSea resulted in more than 1,000 NFTs and BDNs, including amazonwebservices.eth (available for 580 ETH, $2,114,320.40), amazondigitalmarketplace.eth (available for 555 ETH, $ 2,023,185.90), and amazonanalytics.eth (available for 300 ETH, $ 1,093,614.00). Searching for other well-known trademarks led to similar results. For instance, a search for "chanel" on OpenSea results in more than 100 Ethereum BDNs and other NFTs available for sale with the use of different variations of the CHANEL mark, including chanèl.eth (available for 0.009 ETH, $32.81), chanelboy.eth (available for 1 ETH, $3,645.38), and chanelproducts.eth (available for 20 ETH, $72,907.60).[195] However, as of October 2023, most of these listings were deleted and unavailable (although there is no evidence; it might be reasonably related to the right holder's complaints and other attempts by OpenSea to comply with trademark and other laws).

For example, in 2022, OpenSea removed numerous ENS domain auctions following the complaint of the Recording Industry Association of America ("RIAA").[196] In this regard, the RIAA sent a letter to OpenSea identifying that certain music industry-related

---

192 *See, e.g.,* Andrea Calvaruso et. al., *Unauthorized Blockchain Domain Names, supra* note 158*; see also* Registration Data Policy, ICANN, https://www.icann.org/resources/pages/registration-data-policy-2024-02-21-en (last visited Aug. 16, 2024).

193 Kevin Whitley, *Amazon.eth ENS domain owner disregards 1M USDC buyout offer on Opensea*, Cryptoinsiders24 (Sept. 28, 2022), https://cryptoinsiders24.com/2022/07/20/amazon-eth-ens-domain-owner-disregards-1m-usdc-buyout-offer-on-opensea/.

194 *Id.*

195 *Id.*

196 Jack Kubinec and David Canellis, *OpenSea Removes ENS Domain Auctions Following RIAA Complaints*, Blockworks (July 15, 2022), https://blockworks.co/news/opensea-removes-ens-domain-auctions-following-riaa-complaints.

OpenSea-hosted ENS auctions violated U.S. trademark law and, particularly, the ACPA.[197] The list of domain names included such domains as "universalmusic.eth," "atlanticrecords.eth," and numerous other names tied to brands like Columbia Records, Sony Entertainment, and Capitol Records. Also, interestingly, the list of removed ENS domain names included domain names that were based on the personal names of music industry executives like mitchglazier.eth and robstringer.eth (names of the RIAA and Sony Music CEOs, respectively), that are not registered as trademarks. Almost all of these domain names were owned by the same owner (at least, the same blockchain address), who paid between $5 and $15 for the registration of each domain name.[198] In this case, OpenSea complied with the right holder's request and deleted the auctions.[199]

In this regard, BDN providers and Web 3.0. marketplaces, such an OpenSea, claim to take steps to reserve domain names that include well-known names and marks. Also, OpenSea used to have a procedure for removing items from the marketplace in response to a takedown notice from the right holders that was possible to submit via an online form (IP Takedown Request), the link to which is provided in Terms of Use.[200] As of August 16, 2024, the IP Takedown Request Form seems to be inactive and not accessible;[201] however, OpenSea still allows rights holders to report copyright or trademark infringement violations as well as violation of other intellectual property rights via email or physical mail.[202] However, OpenSea has discretion regarding such takedown notices. According to its Terms of Service, a user's access to the OpenSea services is terminated "if the user is determined to be a repeat infringer,"[203] but there are no detailed rules or criteria on how OpenSea determines what practices are considered infringing.

---

197 *Id.*

198 *Id.*

199 *Id.*

200 *OpenSea Terms of Service*, OpenSea (Apr. 4, 2023), https://opensea.io/tos. *See also What can I do if my copyrighted works are being sold without my permission?,* OpenSea, https://support.opensea.io/en/articles/8867068-what-can-i-do-if-my-copyrighted-works-are-being-sold-without-my-permission (last visited Aug. 16, 2024).

201 *What can I do if my copyrighted works are being sold without my permission?*, OpenSea, https://support.opensea.io/en/articles/8867068-what-can-i-do-if-my-copyrighted-works-are-being-sold-without-my-permission ("To request that a collection or item be taken down because you believe that it violates your copyright, please reach out to our Support team.") (last visited Aug. 16, 2024).

202 *OpenSea Terms of Service*, *supra* note 200.

203 *Id.* ("OpenSea will take down works in response to Digital Millennium Copyright Act ('DMCA') takedown notices and/or other intellectual property infringement claims and will terminate a user's access to the Service if the user is determined to be a repeat infringer.")

Other NFT marketplaces provide similar terms, but do not contain comprehensive, user-friendly takedown forms or other procedures to address trademark violations. There are no formalized or harmonized takedown procedures for enforcing trademark rights and fighting cryptosquatting (unlike DMCA copyright notices).[204] Similarly, for BDN providers, there is no unified approach to takedown requests or any harmonized rules regarding trademark protection. Like marketplaces, the measures implemented by BDN providers are very limited, decentralized, and arbitrary. For example, Unstoppable Domains introduced "Protected" status for certain well-known marks (e.g., AMAZON, APPLE, CHANEL, MERCEDES, NETFLIX, etc.).[205] Also, as introduced in 2023, brand owners with proof of ownership can complete a form on the BDN provider Unstoppable Domains to claim ownership of trademarked names to include their brand in Unstoppable Domains' list of "Protected Brands."[206] This is consistent with the Terms of Use of Unstoppable Domains, which provides that customers shall not violate or infringe the rights of others, including intellectual property or other proprietary rights.[207] However, Unstoppable Domains can cancel a domain registration only when the user has not yet "minted" and purchased (i.e., taken) the domain. According to Unstoppable Domains, "Unstoppable Domains does not have the ability to take back trademark domains that were already purchased & minted."[208]

Other BDN providers might have different capacities and approaches.[209] The majority of BDNs providers technically cannot,

---

204 *Id.*; *see also Terms of Service*, Kraken, https://www.kraken.com/legal# (last visited Aug. 16, 2024); *see also Rarible Terms of Service*, Rarible (Dec. 5, 2022), https://static.rarible.com/terms.pdf; *Coinbase NFT Terms of Service*, Coinbase (June 10, 2022), https://www.coinbase.com/legal/nft/terms-of-service; *Binance US Terms of Use*, Binance US (July 30, 2024), https://www.binance.us/terms-of-use.

205 Unstoppable Domains, *supra* note 166.

206 *Protected Brands*, Unstoppable Domains, https://unstoppabledomains.com/tm (last visited Aug. 13, 2024).

207 *Terms of Use*, Unstoppable Domains (Mar. 22, 2024), https://unstoppabledomains.com/terms.

208 Unstoppable Domains, *supra* note 166.

209 *See, e.g.*, *How does ENS work?* ENS, https://support.ens.domains/en/articles/7900417-how-does-ens-work (describing details on ENS registration, "[a]ll .eth names have an expiration date, and in order to maintain ownership of the name, it must be renewed so that it has a valid expiration date."; "[w]hen a new .eth name is registered, the Registrar will also set the Manager in the Registry to the desired address . . . the Manager may be set to a different address, or perhaps the NFT is later transferred to a different address."); *see also* ETH Registrar, https://docs.ens.domains/registry/eth (last visited Aug. 13, 2024) (describing ETH Registrar as a rent-based registrar for the .eth domains).

however, recapture a domain or transfer it to another person (as described above). This is because, unlike traditional Web 2.0 domain names, BDNs are stored on a distributed ledger (e.g., a blockchain) on which "the entry on the blockchain is immutable, meaning it cannot be deleted or changed."[210] In this regard, even a successful takedown of infringing BDNs by NFT marketplaces might not result in an assignment or transfer of those infringing BDNs to the trademark owners. An NFT marketplace, as an intermediary, can only ban the resale of the infringing item on its platform, but intermediaries or even BDN providers themselves cannot transfer or even "burn" the infringing BDN itself (i.e., transfer the domain name to a non-existing address), or at least the "burning" function is available only in very limited circumstances (certain smart contracts might include the option to authorize a third party to "burn" an infringing item).[211]

Considering these technical limitations, some BDN providers limit the sale of BDNs to trademark owners during an initial "sunrise" sale period and provide the brand owners with the ability to add their trademarks to a protected list.[212] In this way, trademark owners who also own their own ICANN TLD have some protection against third-party registrants. What happens, however, when trademark owners do not purchase potentially infringing BDNs before the end of this sunrise period? In that case, others will have access to the registration of these domain names.[213] As discussed above, unlike traditional Web 2.0 domain names, BDNs are stored on a distributed ledge, which makes it challenging even to identify the owner of a blockchain-based domain name, much less to enforce trademark rights against those who own infringing BDNs. Moreover, minting or purchasing just one BDN that operates as a common TLD may potentially lead to the creation of a multiplicity of infringing BDNs that might be further transferred to different owners (in the same way that it happens with Web 2.0 TLDs).[214]

---

210 K. Garbers-von Boehm, *Intellectual Property Rights and Distributed Ledger Technology*, EU Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 43, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/737709/IPOL_STU(2022)737709_EN.pdf.

211 *See, e.g.*, *How does OpenSea handle NFTs with a burn mechanism?*, OpenSea Help Center, https://support.opensea.io/en/articles/8867074-how-does-opensea-handle-nfts-with-a-burn-mechanism (last visited Aug. 13, 2024).

212 *See, e.g.*, *What is a Sunrise Period?*, Pool, https://support.pool.com/hc/en-us/articles/12032812640155-What-is-a-Sunrise-Period- (last visited Aug. 16, 2024) (discussing "an initial list of recognized trademarks/brands that are only available to the trademark holders during our Sunrise period").

213 *Id.*

214 Clare Stouffer, *NFT scams: 10 types + how to avoid NFT fraud*, NortonLifeLock (Feb. 11, 2022), https://us.norton.com/blog/online-scams/nft-scams#; *see also* Megan DeMatteo, *NFT Scams: How to Avoid Falling Victim*, CoinDesk (Aug. 23, 2022), https://www.coindesk.com/learn/nft-scams-how-to-avoid-falling-victim/; *see also* Janos Szurdi, *A Peek into Top-Level Domains and Cybercrime*, Unit 42 (Nov. 11, 2021),

Also, practical risks for brand owners may be compounded if the same TLDs are granted by different providers selling identical blockchain domain names. For example, in October 2022, Unstoppable Domains announced that it decided to "stop supporting .coin domains" as Unstoppable Domains "became aware of a potential collision with our .coin top-level domain and the .coin domain issued by Emercoin, a blockchain platform."[215] As another example, Unstoppable Domains sued Gateway Registry, a company linked with Handshake, over the rights to sell .wallet domains. Unstoppable Domains claimed that "founded in 2018, Unstoppable began commercially using the '.wallet' TLD on Ethereum in June 2021 . . . it has generated over $5,000,000 in revenue from '.WALLET' domain name sales."[216] Although Unstoppable Domains dropped this lawsuit when Gateway Registry stopped selling .wallet domains, similar fights between BDN providers could lead to numerous practical problems for all users and, in particular, for trademark owners, to ensure the protection of their rights.[217]

Handshake, a decentralized, peer-to-peer, permissionless naming protocol, aims to supplant the existing DNS system for ICANN TLDs. To address technical issues relating to its hoped-for transition from the existing ICANN TLD system and to make its new decentralized system backward compatible with the existing ~1,500 ICANN TLDs, Handshake has reserved the existing ~1,500 ICANN TLDs for three years to allow organizations that are already managing ICANN TLD's to claim their TLDs within Handshake's system.[218]

Additionally, currently, BDN providers generally depend on traditional ICANN-controlled Internet services (e.g., for marketing and ensuring access to their services by the general public), and disputes with ICANN-controlled domain name providers pose numerous risks for all stakeholders in Web 3.0. An illustrative example here is the dispute between True Names Ltd. (renamed to ENS Labs, Ltd. in 2023) (responsible for ENS) and GoDaddy (ICANN-accredited domain name registrar) regarding the Web 2.0 domain name eth.link that "acts as a gateway between the

---

https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/.

215 *Why we're no longer offering .coin*, Unstoppable Domains (Oct. 17, 2022), https://unstoppabledomains.com/blog/categories/announcements/article/coin.

216 Unstoppable Domains Inc. v. Gateway Registry, Inc., No. CV 22-948-CFC, 2023 WL 4156709, at *1 (D. Del. June 23, 2023).

217 Andrew Allemann, *Unstoppable Domains drops lawsuit against Gateway Registry*, Domain Name Wire (July 6, 2023), https://domainnamewire.com/2023/07/06/unstoppable-domains-drops-lawsuit-against-gateway-registry/.

218 Ivan Bakalov, *Hosting Handshake domains with DNSimple*, DNSimple Blog (Apr. 26, 2022), https://blog.dnsimple.com/2022/04/introducing-handshake-domain-support/.

traditional 'DNS' namespace and the ENS system,"[219] in other words, "function[s] as a critical bridge that allowed users without Web3-enabled internet browsers to access .eth addresses."[220] ENS Labs alleged that GoDaddy falsely announced to eth.link users that the domain registration had expired and sold the domain to a third party before it was supposed to return to the registry and be available for re-purchase.[221] As of June 2024, the case remains pending; however, on September 9, 2022, the Court granted in part ENS Labs' Temporary Restraining Order and Order to Show Cause for Preliminary Injunction and, in particular, obligated GoDaddy to "immediately transfer ownership in the [d]omain [eth.link] back to Plaintiff."[222] On July 24, 2023, the court ordered the defendant's domain registrar, Dynadot, LLC, to "immediately unlock the domain eth.link, so that Plaintiffs may transfer it to another registrar."[223] It was also ordered that "Plaintiffs may not transfer the [d]omain to a registrar outside the United States and agree not to contest the Court's jurisdiction in entering an Order regarding the disposition of the [d]omain."[224] As of August 14, 2024, the discovery is under way.[225]

To some extent, BDN providers and other stakeholders understand the threat of numerous legal issues, including the threat presented by a potential new wave of cybersquatting in Web 3.0 or, as it might also be called, "cryptosquatting."[226] To address

---

219 Complaint, ENS Labs Ltd. et al. v. GoDaddy Inc. et al. (No. CV-22-01494-PHX-JJTc; D. Ariz) (Dkt. 1 ¶5), LexMachina, https://law.lexmachina.com/cases/2008085631?start=0#docket- [hereinafter *ENS Labs Complaint*] (last visited Aug. 15, 2024).

220 Sandali Handagama, *Eth.link Restored After Ethereum Name Service Wins Injunction Against GoDaddy*, CoinDesk (May 11, 2023), https://www.coindesk.com/policy/2022/09/19/ethlink-restored-after-ethereum-name-service-wins-injunction-against-godaddy/.

221 *ENS Labs Complaint* (Dkt. 1 ¶7-9), *supra* note 219; *see also* Sandali Handagama, GoDaddy Sued Over Sale of Ethereum Domain Name Service's Vital Eth.link Address, CoinDesk (Sept. 8, 2022), https://www.coindesk.com/policy/2022/09/08/firm-behind-ethereum-name-service-and-virgil-griffith-sue-godaddy-over-sale-of-ethlink/?outputType=amp.

222 Order Granting in Part and Denying in Part the Motion for Temporary Restraining Order and Order to Show Cause for Preliminary Injunction (Dkt. 9, Sept. 9, 2022), ENS Labs Ltd. et al. v. GoDaddy Inc. et al., LexMachina, https://law.lexmachina.com/documents/m/235567694 (last visited Aug. 14, 2024).

223 Order Granting in Part and Denying in Part Plaintiffs' Motion to Enforce Preliminary Injunction (Dkt. 77 at 16), https://law.lexmachina.com/documents/m/267066455 (last visited June 15, 2024).

224 *Id.*

225 *See* Notice of Service of Discovery filed by GoDaddy Inc., GoDaddy.com LLC. (Dkt. 94), https://law.lexmachina.com/documents/m/294881566 (last visited June 15, 2024).

226 *See, e.g.*, Kevin T. Dugan, *There's a New Crypto Land Grab Going On*, Intelligencer (Nov. 23, 2021), https://nymag.com/intelligencer/2021/11/ens-domain-squatting-a-new-crypto-land-grab.html; *see also* Jürgen Bebber et al., *From cybersquatting to cryptosquatting: protecting your brand and IP in the era of Web3*, Corrs Chambers Westgarth (Nov. 18, 2022), https://www.corrs.com.au/insights/from-cybersquatting-to-cryptosquatting-protecting-your-brand-and-ip-in-the-era-of-web3; *see also* Holly White, *Web3 Blockchain*

these issues and others, the Web 3.0 Domain Alliance was founded in 2022. The Alliance describes itself as "a member-led, member-driven organization dedicated to improving the technological and public policy environments for users of blockchain naming services"; the Alliance's stated mission includes its "dedicat[ion] to the technological advancement of blockchain domain registries, as well as consumer protection by ensuring the interoperability of blockchain domain registries."[227] The Alliance states that it "believes that blockchain-based generic web3 Top Level Domains . . . developed and marketed by a specific organization are intellectual property, and that industry participants should respect the intellectual property rights of all blockchain naming services for the benefit of consumers as well as applications that want to support blockchain domain functionality."[228] The Alliance has not proposed any specific guidelines related to trademark protection.[229]

2. Legal Barriers for Trademark Protection in Web 3.0

As discussed above, BDNs operate independently from the ICANN network and are not subject to ICANN's rules, including the UDRP, PDDRP, and URS. In other words, BDNs are not subject to the transfer and cancellation remedies available for the trademark owners under UDRP or other ICANN-coordinated procedures.

As for the ACPA, the first hurdle is its applicability to BDNs. The definition of "domain name" under ACPA requires (i) the alphanumeric designation, (ii) that is registered or assigned by (iii) any domain name registrar, domain name registry, or other domain name registration authority, (iv) as part of an electronic address on the Internet.[230] However, most BDNs are purchased or "minted" and owned by the registrants and, in any case, do not involve ICANN-accredited registrars. "Domain name registrars" or "registries" are not defined under the ACPA, however, and the ICANN Glossary and

---

Domain Names: A New Frontier in NFT Brand Protection, Rouse (Oct. 18, 2022), https://rouse.com/insights/news/2022/web3-blockchain-domain-names-a-new-frontier-in-nft-brand-protection ("The web3 domains pose a risk to the brand's image as clients may be misled by impersonating parties. As blockchain domain names have the ability to be used as display names, it is not hard to imagine that users with a display name, such as, 'BrandXOfficial.eth', might mislead other users that they are a brand's official representative.")

227 *See generally* Web 3.0 Domain Alliance, https://www.web3domainalliance.com/ (last visited Aug. 14, 2024).

228 *Id.*

229 According to the information (email) received from the representative of the Web 3.0 Domain Alliance in March 2023, trademark-related guidelines were anticipated to be developed during the summer of 2023, however, no further details were provided, and no guidelines are available as for August 14, 2024.

230 15 U.S.C. § 1127.

applicable regulations require ICANN accreditation for domain name registrars, which is not the case for BDN providers.[231] Finally, BDNs have a different technical nature from DNS, which provides traditional electronic addresses on the Internet. This part of the definition becomes especially controversial considering that the ACPA includes, by reference, a particular definition of the "Internet" as "the international computer network of both Federal and non-Federal interoperable packet switched data networks."[232] Blockchain technologies operate in a substantially different way and do not meet this definition.[233] Therefore, there might be difficulty in applying the ACPA to BDNs and cryptosquatting.

These concerns are also supported by case law on traditional domain names, which tends to limit the scope of "domain name" under the ACPA. Subdomains (i.e., third-level and greater domain names) are not recognized as domain names for the purposes of ACPA actions. For example, in *GoForIt Entm't, LLC v. DigiMedia.com,* the U.S. District Court for the Northern District of Texas considered whether the registration and use of the third-level domain name "goforit.com.org" was subject to the ACPA.[234] The court held that "because under the ACPA a 'domain name' is 'registered with or assigned by' a website registrar, and third-level domains are not registered or assigned, third level domains fall outside the ACPA definition of a 'domain name.'"[235] Ultimately, the court granted summary judgment in favor of the defendant, the registrant of the third-level domain name.[236]

Moreover, no cause of action exists for contributory cybersquatting.[237] Notably, the ACPA does not apply to domain name auction sites.[238] Courts have held that auction websites do not

---

231 *ICANN Glossary, Acronyms and Terms*, Int'l Corp. for Assigned Names & Numbers, https://www.icann.org/en/icann-acronyms-and-terms (last visited Aug. 13, 2024).

232 47 U.S.C. § 230(f)(1).

233 Vasily Agateev and Kseniya Karchenko, *Blockchain or Web3 Domains: Technology, Legal Aspects, Trademarks, and Brand Protection*, Buzko Krasnov (Sept. 7, 2022), https://www.buzko.legal/content-eng/blockchain-or-web3-domains-technology-legal-aspects-trademarks-and-brand-protection; *see also* Dan Patterson, Explaining Web3: From the blockchain and crypto to NFTs and the metaverse, CBS News (Jan. 3, 2022), https://www.cbsnews.com/news/web3-blockchain-crypto-nft-metaverse-explainer/.

234 GoForit Entm't, LLC v. DigiMedia.com L.P., 750 F. Supp. 2d 712 (N.D. Tex. 2010).

235 *Id.* at 724.

236 *Id.* at 743.

237 *See* 6 Callmann on Unfair Comp., Tr. & Mono. § 22:40 (4th ed.) (quoting Petroliam Nasional Berhad v. GoDaddy.com, Inc., 737 F.3d 546, 108 U.S.P.Q.2d 2012 (9th Cir. 2013), *cert. denied*, 135 S. Ct. 55, 190 L. Ed. 2d 31 (2014) (affirming grant of summary judgment to defendant domain name registrar; no evidence supports claim that Congress intended to adopt the common law concept of contributory infringement to cybersquatting; creating such a cause of action would expand liability of domain name registrars inappropriately)).

238 *See* Gilson, *supra* note 54, § 7A.06 (2023).

"traffic" in domain names under the ACPA.[239] For example, in *Bird v. Parsons*, the Sixth Circuit Court of Appeals held that the owner of the mark FINANCIA failed to state a claim, including under the ACPA, against either the registrar or auction service defendants with regard to the domain name "financia.com," because neither the registrar nor auctioneer used the mark.[240] The court held that the defendants' activities of registering the domain name and listing it for auction did not constitute "trafficking" or other "use of" the mark.[241] In this regard, the ACPA has a limited scope, and its direct wording is unlikely to cover BDNs and "mining" operations used to obtain BDNs.

Even applying a broad interpretation of the definition of "domain name" and assuming hypothetically that all ACPA procedures could be used for BDNs, the available ACPA procedures and remedies are not compatible with the nature and functionality of BDNs.[242] In particular, the ACPA provides in *rem jurisdiction*, which refers to jurisdiction over the physical asset (domain name). Still, this tool can be used only in a jurisdiction in which the registrar that issued the domain name is located, and relies on the ability of domain name registrars to transfer or disable domain names.[243] BDN providers might operate their internal governance using the model of a decentralized autonomous organization ("DAO"), an unincorporated association without clear legal status,[244] might be located outside the United States for jurisdictional purposes, might not possess information regarding the owner of the infringing BDN, and, might, in some instances, be impossible for BDN providers to transfer or

---

239 *Id.* (citing Bird v. Parsons, 289 F.3d 865, 878–79, 62 U.S.P.Q.2d 1905 (6th Cir. 2002)) ("[t]he possibility that its customers might buy or sell infringing domain names does not alter the fact that [the auction site] does not use those names."); *see also* Ford Motor Co. v. Greatdomains.com, 177 F. Supp. 2d 635, 644–46, 61 U.S.P.Q.2d 1718 (E.D. Mich. 2001) (finding that auction sites do not "traffic" in domain names nor can they be contributorily liable for cybersquatting).

240 *Bird v. Parsons, supra*, 289 F.3d at 878–79.

241 *Id.* at 869.

242 *See, e.g.*, David H. Bernstein et. al, *You blockhead! Blockchain domain names can cause big grief*, Daily Journal (May 17, 2023), https://dailyjournal.com/articles/372850.

243 15 U.S.C. § 1125 (d).

244 *See, e.g.*, Gail Weinstein et al., *A Primer on DAO*, Harvard Law School Forum on Corporate Governance (Sept. 17, 2022), https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/ ("DAOs . . . are a new kind of entity, regarded by their enthusiasts not as "companies" at all but as collections of individuals organized around the decentralization, autonomous functioning, transparency, and bottom-up principles that characterize the digital universe."); *see also* James Holbein, *Legal Issues Confronting Formation And Operation Of A Decentralized Autonomous Organization (DAO)*, Mondaq (Dec. 09, 2021), https://www.mondaq.com/unitedstates/fin-tech/1140040/legal-issues-confronting-formation-and-operation-of-a-decentralized-autonomous-organization-dao ("The regulators are all struggling to apply well-honed rules for the existing types of hierarchical centralized organizations (banks, stock exchanges, brokers, etc.) to this upstart, decentralized, autonomous, cryptographically-protected new sector that does not fit the current model at all.").

even disable infringing domain names.[245] For example, ENS is governed from Singapore.[246] Also, even if the BDN provider is located in the United States and works through a registration system instead of an ownership system, potential transfers or disabling of infringing BDNs is complicated due to potential challenges to the lack of established enforcement remedies and procedures or other legal measures against cryptosquatting (i.e., as for now, it might not be feasible to adjudicate disputes involving BDNs swiftly and, in even in the case of a successful decision by a court, practical abilities to force the transfer of infringing domain names can be limited).

To illustrate these challenges, it seems helpful to discuss current cases and disputes involving BDNs and more traditional Web 2.0 cybersquatting cases related to Web 3.0 assets. As mentioned above, one of the recent landmark Web 3.0 trademark disputes is *Hermes International et al. v. Rothschild,* which is being litigated in the Southern District of New York.[247] Mason Rothschild created the "MetaBirkins" project, which he hosted at his metabirkin.com and metabirkins.eth domain names, using 100 virtual versions of Hermès BIRKIN handbags that that he offered for sale as non-fungible tokens to users.[248] This project inevitably implicated the trademark rights of the BIRKIN mark owned by Hermès, leading to a trademark infringement and dilution lawsuit.

Hermès asserted the following causes of action[249]:

1. *Trademark Infringement* (unauthorized use of the BIRKIN Mark resulted in Rothschild unfairly benefiting from Hermès' advertising and promotion and profiting from Hermès' reputation and the BIRKIN Mark);
2. *False Designations of Origin* (falsely or misleadingly describing and/or representing the METABIRKINS NFTs as those of Hermès);
3. *Trademark Dilution* (Rothschild's use of the BIRKIN Mark diluted and/or tarnished Hermès mark);

---

245 *See, e.g.*, Unstoppable Domains, *supra* note 166; *see also Kevin T. Dugan*, *supra* note 226.

246 *See, e.g.*, *About ENS*, Ethereum, https://www.exodus.com/news/blockchain-domain-nfts/ [https://perma.cc/V4AN-6JBE]; *see also Frequently Asked Questions*, Ethereum, https://docs.ens.domains/faq (last visited Aug. 21, 2024).

247 Hermes Int'l et al. v. Rothschild, Case No. 1:2022cv00384, CourtListener, https://www.courtlistener.com/docket/62602398/hermes-international-v-rothschild/ (last visited Aug. 14, 2024).

248 *See, e.g.,* Cassell Ferere, *Digital Artist Mason Rothschild Drops 100 'MetaBirkins' NFTs Through Basic.Space*, Forbes (Dec. 13, 2021), https://www.forbes.com/sites/cassellferere/2021/12/13/digital-artist-mason-rothschild-drops-100-metabirkins-nfts-through-basicspace/?sh=71777d4c2000.

249 CourtListener, *supra* note 247, at 34-47.

4. *Cybersquatting* (registration and use of the Infringing Domain caused consumers to falsely believe that the METABIRKINS Website and the infringing METABIRKINS NFTs were affiliated with, endorsed, or approved by Hermès);
5. *Injury to Business Reputation and Dilution* (New York General Business Law);
6. *Common Law Trademark Infringement*; and
7. *Misappropriation and Unfair Competition* (under New York Common Law).

According to Hermès, Rothschild tried to "get rich quick by appropriating the brand MetaBirkins for use in creating, marketing, selling, and facilitating the exchange of digital assets known as non-fungible tokens" and "make his fortune by swapping out Hermès' 'real life' rights for 'virtual rights.'"[250]

Mr. Rothschild moved to dismiss the complaint, arguing that his "MetaBirkins" are artistic works and cited to his First Amendment rights.[251] According to Mr. Rothschild's position, he would prevail on the *Rogers* test, which helps to find the right balance between protecting artistic expression and avoiding likelihood of confusion with a famous mark.[252] However, the court denied Mr. Rothschild's motion, finding that "the complaint sufficiently alleged that the use of the BIRKIN name lacked artistic relevance to the digital images and was explicitly misleading."[253] In February 2023, a jury awarded Hermès $133,000 in damages for trademark infringement, dilution, and cybersquatting.[254] However, after the verdict, as of March 2023, Mr. Rothschild's MetaBirkins website was still active and continuing to promote his MetaBirkin NFTs. In March 2023, Hermès filed a motion seeking a permanent injunction against Mr. Rothschild. Hermès asked to transfer the domain name metbirkin.com (indicated in the complaint as Infringing Domain) and "*any ENS domains* and social media accounts containing the

---

250 *Hermès Complaint*, CourtListener, https://www.courtlistener.com/docket/62602398/1/hermes-international-v-rothschild/, Doc. 1, at *1 (S.D.N.Y. Jan. 14, 2022).

251 *Memorandum of Law in Support of Defendant's Motion to Dismiss*, CourtListener, https://www.courtlistener.com/docket/62602398/17/hermes-international-and-hermes-of-paris-inc-v-mason-rothschild-aka/, Doc. 17 (S.D.N.Y. Feb. 09, 2022).

252 *Hermès Complaint*, *supra* note 250; *Memorandum of Law, supra* note 251; *see also Rogers v. Grimaldi*, 875 F.2d 994 (2d Cir. 1989) (stating that "the use of a trademark in an artistic work is actionable only if the use of the mark: (1) has no artistic relevance to the underlying work, or (2) explicitly misleads as to the source or content of the work.").

253 *Memorandum Order Denying Rothschild's Motion to Dismiss the Amended Complaint*, CourtListener, https://www.courtlistener.com/docket/62602398/50/hermes-international-and-hermes-of-paris-inc-v-mason-rothschild-aka/, Doc. 50, pp. 14-18 (S.D.N.Y. May 18, 2022).

254 *Verdict*, CourtListener, https://www.courtlistener.com/docket/62602398/144/hermes-international-v-rothschild/, Doc. 144, at *1-2, (S.D.N.Y. Feb. 8, 2023).

Birkin mark" to it.[255] Apart from a general reference to the ACPA, 15 U.S.C. § 1125(d)(1)(C), the motion contained no details on the legal grounds or specific ways of transferring an ENS domain name. On June 23, 2023, the court granted a permanent injunction, and barred Mr. Rothschild from "[r]egistering, using, or trafficking any domain names, social media, or NFT platform usernames or handles that use and/or incorporate the 'MetaBirkins' mark."[256] Also, the court ordered Mr. Rothschild to, at his own expense, "[t]ransfer any domain names containing the 'Birkin' mark to Hermès, including 'metabirkins.com.'"[257] The permanent injunction was a win for Hermès and might be likely considered a significant step toward protecting trademark owners against cryptosquatting. However, if Mr. Rothschild violates this court order, due to the nature of decentralized ENS domain names and the lack of settled enforcement mechanisms, Hermès' remedies and practical ways to ensure the transfer of the ENS domain names might be limited, at least without the cooperation of the Ethereum provider. As of June 2024, Mr. Rothschild's appeal is pending before the United States Court of Appeals for the Second Circuit.[258]

Another relevant example is *Yuga Labs Inc. v. Ripps et al.*, where Yuga Labs, creator of the popular Bored Ape Yacht Club ("BAYC") NFTs, claimed that conceptual artist Ryder Ripps infringed Yuga Labs' trademark rights by selling a line of his own NFTs named "RR/BAYC" that used several BAYC trademarks, including the same "BAYC" and "APE" designations used in the domain names "rrbayc.com" and "apemarket.com," Twitter accounts "@ApeMarketplace" and "@ApeMarketBot" and the RR/BAYC smart contract.[259] Although there were no BDNs under consideration, the court analyzed the role of the smart contract underlying BAYC NFTs: "Similar to domain names, smart contracts give consumers confidence in the authenticity and source of digital accounts. As a result, the trademark holder has a superior claim of title to smart contracts bearing its trademarks, particularly in light of the fact that smart contracts are immutable and exist in perpetuity."[260] The court also found that "Defendants' infringing smart contract will always reference Yuga's BORED APE YACHT CLUB and BAYC marks, and, as a result, consumer confusion and harm to Yuga will

---

255 *Hermès Memorandum of Law, supra* note 7.

256 *Order of Permanent Injunction,* CourtListener, https://storage.courtlistener.com/recap/gov.uscourts.nysd.573363/gov.uscourts.nysd.573363.190.0_9.pdf, Doc. 190, at *2 (S.D.N.Y. Jun. 23, 2023).

257 *Id.*

258 Hermes Int'l v. Rothschild, 2d Cir. No. 23-1081, LexMachina, https://law.lexmachina.com/cases/2009534534#docket-entries (last visited June 15, 2024).

259 Yuga Labs, Inc. v. Ripps, No. CV 22-4355-JFW(JEMX), 2023 WL 7089922, at *16 (C.D. Cal. Oct. 25, 2023).

260 *Id.*

continue unabated and in perpetuity . . . [c]onfusion from their infringement will continue unless Yuga Labs owns and controls the smart contract."[261] The court concluded by holding that "it is equitable to order the transfer of the RR/BAYC smart contract to Yuga because Yuga has changed or 'burned' its own BAYC smart contract in order to restrict or prohibit the minting of additional BAYC NFTs in an effort to combat the perceived lack of exclusivity of BAYC NFTs."[262] Overall, the court awarded Bored Ape Yacht Club more than $1.5 million in damages, including the maximum statutory damages for cybersquatting ($200,000 for two domain names at issue), attorneys' fees in the amount of almost $7 million and ordered that all NFTs, social media accounts, and the smart contract in question be transferred to the plaintiff.[263] The defendant complied with the injunction, including the transfer of two Web 2.0 domain names (rrbayc.com and apemarket.com) and the RR/BAYC smart contract, but not the social media accounts or website claiming lack of "possession, custody, or control of the website and Twitter accounts."[264] Also, Ryder Ripps declared that he "destroyed the private keys to any and all cryptocurrency wallets which contains all RR/BAYC NFTs" in his possession, and since the injunction was issued, has not "controlled over any RR/BAYC NFTs."[265]

Interestingly, the analogy between Web 3.0 domain name cases and cases transferring infringing social media accounts might be worth exploring. The legal scholarship includes papers discussing the legal nature of so-called "username squatting" or "username jacking," available remedies, and possible additional remedies.[266] In short, "username jacking" occurs when somebody "creates a social media username identical to or confusingly similar to a brand

---

261 *Id.*

262 *Id.*

263 *Id.* at *21 *("*For all of the foregoing reasons, the Court finds that Yuga is entitled to recover $1,375,362.92 in Defendants' profits, $200,000 in statutory damages, a permanent injunction as described in herein, and its attorneys' fees and costs."); *see also* Karin Segall, *Yuga Labs Awarded over $1.5 million in 'Bored Ape' NFT Dispute*, WTR (Nov. 17, 2023), https://www.worldtrademarkreview.com/article/yuga-labs-awarded-over-15-million-in-bored-ape-nft-dispute.

264 Declaration of Ryder Ripps of Compliance with Injunction, Yuga Labs, Inc. v. Ripps, No. 2:22-cv-04355-JFW-JEM (Dkt. 465 at 4) (Feb. 21, 2024), https://law.lexmachina.com/documents/m/291896671.

265 *Id.*

266 *See generally* Zorik Pesochinsky, *Almost Famous: Preventing Username-Squatting on Social Networking Websites*, 28 Cardozo Arts & Ent. L.J. 223, 225 (2010) (defining username-squatting as "the bad-faith registration of a personal name, other than the registrant's, as a username on a social networking website" and discussing a variety of remedies to fight username-squatting); Dan Malachowski, *"Username Jacking" in Social Media: Should Celebrities and Brand Owners Recover from Social Networking Sites When Their Social Media Usernames Are Stolen?*, 60 DePaul L. Rev. 223, 270 (2010) (discussing the nature of username jacking and available remedies).

owner's trademark or service mark and subsequently uses that social media account with a bad faith intent."[267] Also, it may occur in the case of bad-faith use of "the personal name, particularly of a well-known or famous individual."[268] The debate regarding the potential remedies against username squatting practices usually includes an analogy with domain names and a discussion of the ACPA-UDRP framework.[269] In the meantime, there is a substantial disagreement about whether the ACPA/UDRP-like framework could be applicable to usernames, due to differences in the nature and primary focus on personal name protection (e.g., protection against defamation, identity theft, or privacy/publicity violations).[270] Also, practice shows that username squatting can usually be addressed by takedown procedures without initiating court or other enforcement proceedings.[271] Major social media companies are likely interested in protecting their users against username jacking and have developed methods to help users combat username squatting on their platforms (e.g., Instagram's Terms of Use and Trademark Request Form specifically allow claims to an infringing username and provide for the transfer of it to the right holder).[272] Therefore, the analogy between BDNs and social media usernames, although interesting to discuss, is not very helpful for the purposes of this article.

Unlike most social media providers or Web 2.0 domain names, there are no specific practical or legal mechanisms to facilitate the transfer of BDNs to a trademark owner or alternative procedures to stop trademark infringements. As discussed above, current takedown procedures are limited, and primarily relevant to stopping the resale of infringing content in the marketplaces, but not to the BDN providers who mint and operate BDNs. Even a court order to a BDN provider to transfer an infringing BDN, like the

---

267 Brian A. Hall, Mallory King, *What Is Social Media Squatting and Is It Time to Legislate?*, The Brand Prot. Pro. (Mar. 2020) https://bpp.msu.edu/magazine/what-is-social-media-squatting-and-is-it-time-to-legislate-march2021/.

268 *Id.*

269 Pesochinsky, *supra* note 266 ("This Note proposes a solution to the username-squatting problem by using the ACPA and UDRP as models, analyzing what factors should be borrowed from the domain name resolution mechanisms and how the borrowed factors should be applied in the username context."); *see also* Daniel Doft, *Facebook, Twitter, and the Wild West of IP Enforcement on Social Media: Weighing the Merits of a Uniform Dispute Resolution Policy*, 49 J. Marshall L. Rev. 959, 967-72 (arguing for the creation of the Uniform Social Media Intellectual Property Dispute Resolution Policy).

270 *See, e.g.*, Malachowski, *supra* note 266, at 268 (arguing that "[c]ybersquatting laws should not apply to usernames because the ACPA covers domain names, not sub-domains like Facebook vanity URLs and Twitter handles.").

271 *Id.* (arguing that "the large majority of username-jacking situations should be resolved without the involvement of the courts" and that "[s]ocial sites do enough to prevent username jacking.).

272 *Trademark Report Form*, Instagram, https://help.instagram.com/contact/230197320740525 (last visited Aug. 16, 2024).

injunction mentioned in *Hermes International et al. v. Rothschild,* is almost impossible to enforce when the BDN provider does not cooperate and/or is located outside of the Court's jurisdiction. Moreover, as explained above, due to the nature of BDNs (as an unalterable entry on the blockchain), the transfer or even "burning" of the infringing BDN is not always technically possible, even for BDN providers.

Furthermore, trademark owners face challenges even to identify the owner of an infringing BDN, much less to establish that a domain name registration was made in bad faith for the purpose of reselling the BDN. While the Web 3.0 world is still developing, there are a number of such cases involving Web 2.0 domains. In particular, numerous Web 2.0 domain names that include third-party trademarks in combination with Web3-related terms like "NFT" and "metaverse" (e.g., nftwhatsapp.com, nftmorganstanley.com, louisvuittonnft.com, lego-metaverse.com, nft-lego.com, and nftsinstagram.com) have been transferred to the trademark owner through the UDRP's procedures. For example, the domain name nftmorganstanley.com was registered by a person unrelated to Morgan Stanley. In the UDRP dispute initiated by Morgan Stanley, the UDPR panel determined that the domain name was confusingly similar to the trademark owned by the financial services firm (Morgan Stanley).[273] The UDRP panel found that the registrant of the nftmorganstanley.com domain name had no rights or legitimate interests in it and that it registered and used the domain name in bad faith.[274] With respect to showing bad faith, the panel noted that competing pay-per-click links may indicate bad faith.[275] After evaluating the facts, the panel ordered the domain name to be transferred to Morgan Stanley.[276] As in all cybersquatting cases, it is essential to demonstrate a lack of the registrant's rights or legitimate interests in the disputed domain

---

273 Morgan Stanley v. Joseph Masci, Nat'l Arb. Mediation Int'l Forum (Sept. 25, 2021), https://www.adrforum.com/domaindecisions/1940938.htm; *see also* WhatsApp, LLC v. Domain Admin, Isimtescil.net / Whoisprotection.biz / Mohammed Alkurdy, Evan Digital Technology Group, Case No. D2021-2329, WIPO (Oct. 12, 2021) (transferring domain names "nftwhatsapp.click," "nftwhatsapp.com," "nftwhatsapp.net," "whatsappnft.click," "whatsappnft.com," and "whatsappnft.net"); *see also* Louis Vuitton Malletier v. Niko Porikos, Case No. D2022-4097, WIPO (Jan. 2, 2023) (transferring the "louisvuittonnft.com" domain name); LEGO Juris A/S v. Oleg Kovalev, Case No. D2022-1993 (WIPO Aug 4, 2022) (transferring the "lego-metaverse.com" and "nft-lego.com" domain names); Instagram, LLC v. Adam Lee, Case No. D2022-2908 (WIPO Sept. 27, 2022) (transferring the domain names "instagramsnft.com," "instagramnfts.com," "nftinstagrams.com," and "nftsinstagram.com").

274 *Morgan Stanley*, *supra* note 273.

275 *Id.*

276 *Id.*

names and to provide evidence of bad faith registration.[277] Adding the acronym of the descriptive term NFT to an existing trademark does not obviate a finding of confusing similarity, and such a domain name may very well be transferred to the trademark owner.[278]

However, the described UDRP procedures are unavailable for Web 3.0 domain names. In this regard, if somebody purchases in bad faith domain names like "whatsapp.nft" or "morganstanley.eth," the only remedy for the trademark holder to recover these domain names is to investigate the identity of the owner of these domain names and to initiate a trademark infringement, dilution, or cybersquatting action in court, which can be additionally complicated by the jurisdictional issues and the user-ownership model implemented by numerous BDN providers.

Overall, the current situation with respect to BDNs resembles the pre-ACPA/UDRP Web 2.0 stage when trademark owners and courts struggled with cybersquatting, such as in Toeppen's cases in the 1990s.[279] Therefore, there is a need for laws such as the ACPA to be reexamined or at least reinterpreted to allow for the enforcement of trademark rights with respect to BDNs (to the extent it is technically possible, for example, when the BDN providers have rights to cancel the registration of BDNs.[280] Moreover, at the global level, it might be beneficial to develop new flexible UDRP-like dispute resolution mechanisms applicable to BDNs.

PART III. A CALL FOR A NEW REGULATION: PROTECTING TRADEMARKS AGAINST CRYPTOSQUATTERS

In light of the challenges articulated above, it is essential to develop legal mechanisms to address the bad-faith registration and use of BDNs worldwide. It is important to employ a combination of instruments considering the interests of the relevant stakeholders. In particular and considering the experience of cybersquatters in Web 2.0 and the strong public interest in preventing cryptosquatting in Web 3.0, it seems reasonable to focus primarily on legislative measures and international dispute resolution procedures.

---

277 Uniform Domain Name Dispute Resolution Policy, Section 4(b), https://www.icann.org/resources/pages/policy-2012-02-25-en (establishing the standard for the use of the "evidence of registration and use in bad faith.").

278 *See, e.g., Morgan Stanley, supra* note 273; *see also WhatsApp, supra* note 273.

279 *Toeppen,* 947 F. Supp. 1227; *Toeppen*, 141 F.3d 1316, *supra* note 30.

280 *See e.g., How does ENS work*?, *supra* note 209 (discussing the rental principle beyond .eth domains); *see also Terms of Use*, Unstoppable Domains, *supra* note 207 (discussing that BDNs might be only canceled before they minted).

A. Proposals to Amend the U.S. Laws to Address Cryptosquatting

1. Proposals to Amend the ACPA

Among other things, it seems relevant to ensure the applicability of the ACPA mechanisms to U.S.-related BDN disputes. Although some ACPA remedies might be inapplicable due to the nature of blockchain technologies and the technical impossibility for some BDN providers to transfer or disable certain BDNs, the basic framework and general remedies, such as monetary damages and injunctions, can still be applicable and relevant to fight cybersquatting in Web 3.0.

As noted by experts of the American Bar Association Section of Intellectual Property Law, "any amendment or supplement to laws such as the ACPA will need to explore the degree to which the immutable nature of blockchain technologies has an impact on enforcement options (such as takedown, transfer, etc.) once an alleged or actual infringement is found."[281] Indeed, to regulate BDNs in an orderly and fair manner, it is essential to account for differences in how BDNs are created, maintained, and administered.

As a first step, it is essential to amend the definition of "domain name" to incorporate BDNs or to develop a specific legal definition of BDN and, in this way, to apply the ACPA to BDNs. For example, a domain name might be defined as "a unique alphanumeric designation that is registered, assigned, or otherwise transferred by a domain name registrar, domain name registry, or other domain name registration authority, any other organization, or individual, and that is used to identify a specific location on the Internet, including alternative web systems." Alternatively, a blockchain-based domain name might be defined as "a unique alphanumeric designation that is registered, assigned, or otherwise transferred by a blockchain-based domain name registrar, registry, any other organization, or individual, and that is used to identify a specific location on a distributed ledger." Also, it is appropriate to provide right holders with a broad range of ACPA remedies as well as to develop BDN-specific remedies giving infringers a set amount of time to transfer an infringing BDN and, in case of a lack of compliance, imposing specific monetary fines and/or criminal penalties. These proposals, in combination with other measures discussed above (including contractual-based measures, self-regulation, and further development of various technological measures against cryptosquatting), would be critical in developing a proper legal regime for BDNs. In the meantime, a wide-ranging discussion with the participation of technical specialists and

---

[281] *Roger LaLonde et al.*, *supra* note 179.

government representatives might be constructive and lead to the development of detailed and balanced amendments to the ACPA.

2. Secondary Liability: Assessing the Scope of the Liability of BDN Providers

Organizations and individuals engaged in the sale or use of BDNs should not be able to avoid legal responsibility when they enable, encourage, or promote infringing activities. It should be made clear that BDN providers can be liable in cases when the provider has (directly or indirectly) a "bad faith intent to profit" from a third party's trademark and enables, encourages, or promotes a registrants' infringing activities (that is more than just providing registration or support general services to those register BDNs without being specifically put on notice regarding the infringing activity). This approach generally corresponds with the current approach of U.S. courts to secondary liability, but its further clarification and to some extent further development and unification might be helpful.

A finding of secondary liability in trademark cases is based on those common law principles aimed at determining whether the contributor is liable: (1) when he "intentionally induces another to infringe on a trademark" or (2) when he "continues to supply its product to one whom [he] knows or has reason to know is engaging in trademark infringement . . . ."[282] Under the case law relating to Web 2.0. domain name registrars, courts tend to limit the secondary liability of domain name registrars, noting that "allowing suits against registrars for contributory cybersquatting would not advance the goals of the ACPA"[283] and that "extending liability to registrars or other third parties who are not cybersquatters, but whose actions may have the effect of aiding such cybersquatting, would expand the range of conduct prohibited by the statute."[284] Overall, in Web 2.0, secondary liability of domain name registrars is limited to cases where registrars (i) register, use, or traffic in the domain name with a bad faith intent to profit, or (ii) have engaged in wrongful conduct that surpasses mere registration activity.[285]

---

[282] Inwood Lab'ys v. Ives Lab'ys, 456 U.S. 844, 854 (1982); *see also Liability Under the ACPA*, *supra* note 28, at 337.

[283] *Petroliam, supra,* 737 F.3d at 548.

[284] Rigsby v. GoDaddy Inc., 59 F.4th 998, 1006 (9th Cir. 2023) (quoting Petroliam, 737 F.3d at 550).

[285] *See, e.g.*, *id.* 59 F.4th at 1003 ("As to the Lanham Act claim, the panel further held that Rigsby could not overcome GoDaddy's immunity under the Anticybersquatting Consumer Protection Act, which limits the secondary liability of domain name registrars and registries for the act of registering a domain name. The panel concluded that Rigsby did not plausibly allege that GoDaddy registered, used, or trafficked in his domain name with a bad faith intent to profit, nor did he plausibly allege that GoDaddy's alleged wrongful conduct surpassed mere registration activity.").

On the one hand, this limitation on the liability of domain name registrars seems logical and helps registrars conduct their business without being exposed to constant complaints from trademark owners. Also, as noted by courts, "because direct cybersquatting requires subjective bad faith, focusing on direct liability also spares neutral third-party service providers from having to divine the intent of their customers."[286]

On the other hand, the value of this limitation on secondary liability is debatable, even with respect to Web 2.0 domain name registrars,[287] and needs to be reassessed with regard to BDN providers whose "neutral" status with respect to trademark violations might be more arguable in light of the current model of selling BDNs without ensuring sufficient—or any—protection for trademark owners, such as providing efficient mechanisms to address cryptosquatting. Moreover, BDN provider's sales of BDNs might go beyond providing registration services because a BDN provider might transfer ownership of an infringing domain name to a registrant. Interestingly, some BDN providers organize promotions and competitions, allowing users to mint BDNs without knowing the identity of the domain names that they purchase, much less their value.[288]

In this regard, secondary liability for trademark infringement is generally applicable with respect to BDN providers, and a wider and more unified understanding and approach might turn out to be helpful. Since courts have not elaborated on the specific criteria and limitations on the liability of BDN providers and considering other struggles with the liability of domain name registrars and resellers of Web 2.0 domain names,[289] which causes uncertainty for all stakeholders, it seems appropriate to consider amending the ACPA to clarify these criteria and limitations. By amending the statute, there can be unified liability criteria for all types of intermediaries that would result in a more predictable and settled case law with respect to the secondary liability of both Web 2.0 and BDN providers.

---

286 *Petrolia, supra,* 737 F.3d at 553.

287 There are numerous comments claiming that the secondary liability of domain name registrars should be strengthened. *See, e.g.*, *Liability Under the ACPA*, *supra* note 28, at 337; *see also* Nicholas F. Barbantonis, Should Contributory Cybersquatting Be Actionable?, 17 N.C. J.L. & Tech. 79, 89-90.

288 *See, e.g.*, *Introducing Magic Boxes with Magic Eden*, Unstoppable Domains (April 10, 2023), https://unstoppabledomains.com/blog/categories/announcements/article/magic-eden-mystery-box?utm_campaign=2023.4.13-General-Newsletter-A&utm_content=2023.4.13-General-Newsletter&utm_medium=lifecycle_email&utm_source=lifecycle_UD ("Each Mystery Box will cost $100 (also payable in MATIC) and contains an Unstoppable domain valued at least $100 inside.").

289 *See, e.g.*, Baraa Kahf. *Congress Should Rescue the ACPA From Irrelevance*, Law360 (Sept. 7, 2022), https://www.law360.com/articles/1525039.

B. Certain Considerations Regarding International Regulations

1. Foreign Laws and Potential International Laws Addressing Cryptosquatting

As described in Parts 1 and 2, cybersquatting in Web 2.0 and cryptosquatting in Web 3.0 have an international nature, and, in this regard, it is worth discussing potential amendments to foreign laws and the development of possible international solutions to address cybersquatting.

Countries that have adopted statutes addressing cybersquatting, such as Belgium, Norway, and Nigeria can potentially follow the same approach as suggested for the U.S. and modify their statutes to incorporate cybersquatting directly. In the meantime, as analyzed above, most countries do not have national laws addressing cybersquatting, and what laws do exist provide different approaches to addressing cybersquatting. The concept of secondary liability and the intermediaries' approaches to liability are also not harmonized.[290] In this regard, legal measures at the international level aimed to harmonize and develop balanced anticybersquatting regulations should be undertaken.

Since the 1990s, the international community has discussed different approaches to fighting cybersquatting, including the development international treaties, the creation of special dispute resolution systems corresponding to existing international treaties (e.g., the Madrid Agreement), and the drafting of a Model Law on Cybersquatting.[291] Some of these ideas might also be worth

---

290 *See, e.g.*, Gerlinde Berger-Walliser and Kurt Saunders, *The Liability of Online Markets for Counterfeit Goods: A Comparative Analysis of Secondary Trademark Infringement in the United States and Europe* (Mar. 22, 2011) ("All stakeholders would greatly benefit from a more uniform judicial assessment of online service providers' secondary trademark infringement liability by different national courts, as such uniformity would lead to greater legal certainty. In civil law countries, such as Germany and France, where the freedom of courts to create law is limited, the issue ultimately can only be resolved by the legislator. In contrast, in common law systems, such as the U.S. and the U.K., a standard of secondary liability can be judicially fashioned, as indeed it was by the U.S. Supreme Court in the Inwood case."), https://www.researchgate.net/publication/228280232_The_Liability_of_Online_Markets_for_Counterfeit_Goods_A_Comparative_Analysis_of_Secondary_Trademark_Infringement_in_the_United_States_and_Europe; *see also* Mostert and Schwimmer, *supra* note 115, (stating that "current uncertainty and lack of consistency on the legal treatment of trademarks and intermediary liability on an international basis"); *see also* Stacey L. Dogan, Intermediary Trademark Liability: A Comparative Lens, JOTWELL (May 28, 2014), (reviewing Graeme B. Dinwoodie, Secondary Liability for Online Trademark Infringement: The International Landscape, 36 Colum. J.L. & Arts), https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1078&context=shorter_works.

291 *See, e.g.*, Rodney A. Meyer, *Domains without Borders: Reconciling Domain Name Dispute Resolution Policies and Trademark Rights between the United States and the Nations of the European Union*, 20 Penn State Int'l L. Review 415, 437 (2002), http://elibrary.law.psu.edu/psilr/vol20/iss2/6 ("[U]nder the system proposed in this

revisiting in connection with Web 3.0 domain names. For example, James Plotkin, in his work "A Proposal for a Model Law Dealing with Cyber-Squatting" advocates for the development of a model law on cybersquatting that countries might adopt and apply in a uniform way.[292] In Plotkin's vision, the proposed model law could be "capable of working in tandem with the UDRP," while being "superior to the UDRP" at the same by creating "an exhaustive legal regime under which no reference need be made to trademark law."[293] In the meantime, Plotkin recognizes that "[l]ike any international instrument, a model law is only useful if it is implemented" and that "[s]ince the U.S. already has the ACPA, it would likely not sign onto the model law."[294] Also, "[g]iven that U.S. courts have demonstrated a willingness to exercise extra-territorial jurisdiction when it comes to domain names, the effect of the model law may be attenuated."[295]

In this regard, harmonized rules for all Web 2.0 and Web 3.0 players worldwide seem to be desirable, and the idea of developing a particular international regulation, such as the proposed model law, looks appealing. Focusing on practical considerations and the difficulties with negotiating and enforcing such international regulations as model laws, however, suggests that this approach might not be as fruitful as desired. Moreover, experience has shown that a contractual-based approach to regulating domain names in Web 2.0 is a working and flexible enough instrument to help to establish uniform rules and procedures worldwide.

---

comment, the potential domain name registrant will not receive a domain name registration until it has been determined that no trademark holder within the Madrid System is waiting in the shadows to come forth and take the domain name away."); *see also* James Plotkin, *The Model for a Path Forward: A Proposal for a Model Law Dealing with Cyber-Squatting and Other Abusive Domain Name Practices*, 27 Denning L. J. 204, 205 (2015), https://canlii.ca/t/sl18 ("The proposed solution represents a major change to the current cyber-squatting framework a model law dealing with cyber-squatting and other abusive domain name practices. This purpose-built piece of model legislation would create causes of action for cyber-squatting and what is known as reverse-domain name hijacking, the practice of instituting false cyber-5 squatting claims to have a domain name transferred from a registrant.").

292 Plotkin, *supra* note 291.

293 *Id.* at 239 (clarifying the following benefits of the proposed model law, "decisions invoking the model law are final; it eliminates the propensity for bias inherent in the complainant/provider-driven UDRP panel selection process; the greater variety in legal background of judges eliminates the pro-intellectual property slant some UDRP panelists may carry; it provides robust protection against reverse-domain name hijacking; it captures passive warehousing; it protects personal names; and it will not conflict with national consumer protection and language laws.").

294 *Id.* at 234.

295 *Id.*

2. International Contractual-based UDRP-like Rules and Procedures for BDNs

Considering the above-mentioned challenges and possible responses, one promising measure to combat cryptosquatting in Web 3.0 might be to develop a UDPR-like policy specifically for BDNs, e.g., Uniform Blockchain Domain Name Dispute Resolution Policy ("UBDRP") or adjusting current UDRP procedures to ensure legal and practical applicability to BDNs.

The idea beyond the development of the UBDRP is to provide a fast, cheap, and transparent process for trademark owners to challenge the registration and use of BDNs that are identical or confusingly similar to their trademarks. Also, and consistent with the UDPR, it seems reasonable that a UBDRP would be consistent with the principles and provisions of international trademark law and have an international application. UBDRP procedures could be administered by a neutral third party, such as the World Intellectual Property Organization (WIPO), allowing for appeals to national courts.

Moreover, to develop and ensure the efficient nature of a UBDRP, it might be helpful to have an organization or alliance to oversee this process, or partner with ICANN to use ICANN's resources to develop the applicable legal procedures and framework. Similar reasoning and initiatives apply to this proposal as those that supported the development and implementation of the UDRP. As noted in the International Association for the Protection of Intellectual Property ("AIPPI") report regarding the UDRP and global domain name disputes, "the system should probably provide for accountability mechanisms, including minimal involvement of the government as a regulator and independent review."[296] For example, Web 3.0 Domain Alliance members might already have taken steps to protect users' identities and prevent fraud or naming collisions within Web 3.0. They may also be willing to work together towards alignment on intellectual property rights for all Web 3.0 naming services and how best to avoid consumer harm.[297] In the meantime, cooperation with ICANN and government departments and agencies, including the U.S. Department of Commerce (as was the case with ICANN and UDRP in 90-s[298]), might also be needed

---

296 *Issues of co-existence of trademarks and domain names: public versus private international registration systems*, Int'l Assoc. for the Prot. of Intell. Prop. (July 15, 2003), https://aippi.soutron.net/Portal/Default/en-GB/RecordView/Index/2873.

297 Nora Chan, *Web 3.0 Domain Alliance Launches to Protect Users' Digital Identities*, The Daily Hodl (Nov. 2, 2022), https://dailyhodl.com/2022/11/02/web-3-0-domain-alliance-launches-to-protect-users-digital-identities/.

298 *See, e.g.*, Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy"—Causes and (Partial) Cures*, 67 Brook. L. Rev. 605 (2002), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1681&context=blr; *see also* ICANN's Relationship with the

and beneficial to ensure the legality and safety of the BDN system as well as their coexistence with the DNS domain system. This initiative becomes especially relevant in light of the development of interoperable domain names aimed to bridge the worlds between Web 2.0 and Web 3.0.[299] Further development of such interoperable domain names would substantially benefit from having unified procedures applicable to their registration and use.

Additionally, it seems reasonable to involve private and public stakeholders in developing a UBDRP or adjusting current UDRP procedures to make UBDRP a part of current UDRP procedures. Such stakeholders might include governments of various countries, leading international organizations in the area of the Internet and Intellectual Property Law (e.g., AIPPI, ICANN, WIPO, INTA, etc.), industry representatives (i.e., BDN providers, marketplaces, etc.), and trademark owners. In particular, it might be beneficial if international organizations focusing on intellectual property law and policy were to conduct a study on the views of different jurisdictions on the proper legal framework for BDNs and to provide suggestions regarding dispute resolution procedures. These measures could provide a fair, flexible, and efficient mechanism for resolving disputes between BDN registrants and trademark owners without being unduly burdensome on either trademark holders or domain name registrants.

Overall, developing a UDPR-like policy for BDNs seems to be a helpful, practical mechanism to resolve BDN-related trademark disputes. The flexibility of UDRP-like ADR procedures seems to be beneficial for all stakeholders in Web 3.0 and will support the twin aims of protecting trademark owners from cybersquatting while affording BDN owners with appropriate due process rights. The UBDRP framework proposed herein might become such a mechanism, but its final version should be developed with the engagement of stakeholders worldwide.

C. Other Remedies and Self-regulation Initiatives in Web 3.0

To ensure the balanced development of Web 3.0 and an efficient global system of BDN registration, it is essential to create a fair and safe Web 3.0 environment for all stakeholders. To achieve this, it is important to consider all conflicting interests and to allow BDN providers to be involved in developing regulations related to BDN registration and resale.

To some extent, these self-regulatory initiatives are already being developed by some stakeholders, including by the Web3

U.S. Government, ICANN, https://www.icann.org/resources/pages/history-resources-usg-2017-05-04-en (last visited Aug. 15, 2024).

299 *See, e.g.*, *Web3 Innovation, supra* note 6; *see also Web2+Web3, supra* note 163.

Domain Alliance, "a member-led, member-driven organization dedicated to improving the technological and public policy environments for users of Web3 naming services."[300] The Web3 Domain Alliance is dedicated to developing "the functioning of Web3 domain registries with and across blockchain-based and traditional web applications" and "improving the technological and public policy environments for users of blockchain naming services."[301] It is working to develop technical standards, policies, and guidelines for industry members.[302] Although the Alliance's efforts are still in their early stages, such efforts to create a safe and responsible environment for using BDNs seem to be beneficial for all stakeholders, including the potential for being a leading actor in creating and administering UDRP-like procedures for BDNs and other regulations for all Web 3.0 players. In particular, it is valuable that the Alliance is already working on intellectual property protection policies and other relevant rules to protect users from fraud and abuse and to ensure transparency, accountability, and responsibility for all members of the Web 3.0 industry.[303]

Interestingly, in November 2023, a separate Asia Web 3 Alliance was founded to "construct a collaborative ecosystem across 48 countries with Japan, Asia, and the world."[304] Specifically, Asia Web 3 Alliance was established with "the aim of globally advancing Japan's Web3 industry and attracting foreign investors to the Web3 ecosystem in Japan and Asia."[305] As for now, the agenda of this Alliance does not explicitly include the protection of intellectual property.

From a global perspective, it might be helpful to include stakeholders from all over the world in the dialogue regarding such a framework, as it is beneficial—if not necessary—to ensure the cooperation and involvement of international representatives, especially those from the Web 3.0 industry and leading trademark owners. Collaboration between various international alliances can help to address many of the issues relating to BDNs, including intellectual property protection and transparency in internal policies and terms.

---

300 The Web3 Domain Alliance, https://www.web3domainalliance (last visited Aug. 14, 2024).

301 *Id.*

302 *Id.*

303 *Id.*

304 Rita Carvalio, *Launch of 一般社団法人ASIA WEB3 ALLIANCE JAPAN Promises to Construct a Collaborative Ecosystem Across 48 Countries with Japan and Asia*, Fab World Today (Dec. 11, 2023), https://www.msn.com/en-us/news/other/launch-of-%E4%B8%80%E8%88%AC%E7%A4%BE%E5%9B%A3%E6%B3%95%E4%BA%BAasia-web3-alliance-japan-promises-to-construct-a-collaborative-ecosystem-across-48-countries-with-japan-and-asia/ar-AA1lqCwW.

305 *Id.*

Another relevant mechanism to protect trademark owners might be to create a global public registry of BDNs. Similar to the pre-GDPR WHOIS, such a registry could include information on the ownership of BDNs and relevant restrictions and/or limitations on their use. To some extent, Freename.io, a Web 3.0 registrar, is already working on this initiative, and has created a so-called Web3 WHOIS.[306] As claimed by Freename.io, "Web3 WHOIS is the twin of WHOIS in Web 2.0, the tool used to look up information about domain and IP owners and check dozens of other statistics: users can get all the data about a domain and everything associated with that domain at any time with a single search."[307] The development of such a registry is a constructive initiative, but this registry must be scalable and reliable and incorporate data from all of the relevant BDN providers.

Moreover, it might be helpful if the stakeholders were to create a system for reporting and addressing BDN abuse, including cryptosquatting, and a process for investigating and addressing any such reports. This system could allow trademark owners to report incidents uniformly and relatively quickly without requiring them to engage in official enforcement procedures.

Some initial attempts to create a system for identifying and reporting cryptosquatting are being implemented by private brand monitoring systems. For example, Corsearch launched an NFT monitoring and enforcement solution to help streamline IP protection within the metaverse.[308] As described by Corsearch, five major NFT marketplaces are covered, and Corsearch aims to add more: OpenSea, Rarible, Mintable, Super Rare, and Foundation.[309] The platform also provides semi-automated enforcement with high compliance and data-driven reporting to inform a company's NFT strategy.[310] Interestingly, the website states that "while OpenSea's IP enforcement protocols aren't always clear, Corsearch has a good relationship with the platform, meaning infringement notices are actioned within just hours."[311] Similar services are provided by the Com Laude platform, which has created a blockchain domain registration and management program.[312] Com Laude claims to

---

306 *Freename Launches the First WHOIS for Web3 Domains*, Freename (Jan. 2, 2023), https://www.newsfilecorp.com/release/150028/Freename-Launches-the-First-WHOIS-for-Web3-Domains.

307 *Id.*

308 *Brand Protection in the Metaverse: What Brands Need to Know*, Corsearch (Nov. 15, 2022), https://corsearch.com/content-library/blog/brand-protection-in-the-metaverse-what-brands-need-to-know/.

309 *Id.*

310 *Id.*

311 *Id.*

312 *Web 3.0 Services including Blockchain Domains*, Com Laude, https://comlaude.com/services/web-3-0-blockchain-domains/ (last visited Aug. 14, 2024).

cover the most popular blockchains, such as Unstoppable, Ethereum, and Handshake, as well as certain local markets.[313] Com Laude helps trademark owners with BDN registrations, risk assessment, and management of BDNs.[314] Markmonitor also claims to "provide a broad range of NFT domain solutions catered to corporate brands and their needs in this space" using its "developed relationships with Web3's most prominent NFT Domain Registries and other Web3 security partners."[315] These measures and services are limited, however, and depend on the participation and cooperation of BDN marketplaces and providers.

In the meantime, "the number of different providers offering different models is increasing, and this escalates the challenges with name collisions, brand or trademark infringement, and abuse through use cases."[316] In this regard, "unity between Blockchain Domain Providers is critical,"[317] and it becomes crucial for stakeholders, primarily BDN providers and the marketplaces themselves, to be actively involved in the harmonization of BDN-related brand protection policies and mechanisms. In particular, it can be done via dedicated programs, task force groups, and forum discussions held on the platforms of dedicated associations such as the Web3 Domain Alliance or major intellectual property associations (e.g., WIPO, IAPPI, INTA, etc.).

Of course, it goes without saying that any procedures to address cryptosquatting must be created and implemented only after careful discussion with IT, security specialists, and relevant stakeholders. Also, in light of the discussions about interoperability and potential application with ICANN for Web 3.0 domain names,[318] further research and discussions involving ICANN, based on the best Web 2.0 practices, might be helpful in establishing a proper framework for Web 3.0, both with respect to technical aspects (prevention of name collision, interoperability, etc.) and with respect to legal issues (in particular, trademark protection and anticybersquatting mechanisms).[319]

---

313 *Id.*

314 *Id.*

315 *Web 3 Solutions*, Markmonitor, https://www.markmonitor.com/web3-nft-domains/ (last visited Aug. 14, 2024).

316 *Web3 disruption*, *supra* note 10, at 160.

317 *Id.*

318 *See, e.g.*, *Web3 Innovation, supra* note 6.

319 *Id.* (stating that "ICANN Participation or Involvement is needed to ensure these challenges are adequately addressed. Name collisions are a concern with the next round of TLDs expected and multiple name collisions already exist. The ability to bridge blockchain domain names and DNS mean that ICANN needs to participate in the discussion. They should adopt a pragmatic approach towards blockchain domain names.").

Ensuring cooperation between different stakeholders worldwide, increasing and diversifying stakeholder involvement,[320] and adopting a combination of regulatory and technical mechanisms is likely to be the most effective way to address cryptosquatting and to provide a clear set of remedies for trademark owners holders, while balancing the interests of Web 3.0 participants.

CONCLUSION

This article explored trademark-related international challenges arising in Web 3.0, specifically focusing on trademark protection against cryptosquatting, i.e., cybersquatting in Web 3.0 consisting of the bad faith registration and use of BDNs that are identical or confusingly similar to existing trademarks.

Analysis of the current regulatory framework, including the ACPA and UDRP, helps to understand the development, core principles, advantages, and disadvantages of the current Web 2.0 anti-cybersquatting regulatory system. Overall, the ACPA-UDRP framework and other ICANN-related tools provide a relatively effective mechanism to protect trademark rights in Web 2.0.

The rise of Web 3.0 and the constant growth of the BDN industry demonstrate the need to rethink existing anti-cybersquatting mechanisms and to adapt them to address cryptosquatting in the Web 3.0 world. Currently, remedies for trademark owners are mostly limited to pre-Internet trademark dilution claims and attempts to file takedown notices and establish secondary liability for BDN providers.

As noted in the INTA White Paper "Trademarks in the Metaverse," "with the growth of NFTs and their potential use as domains, there is a compelling need for the legal and consumer protection community to lobby for enforcement mechanisms and policies to prevent illegitimate use of trademarks as blockchain domains."[321] Indeed, there is a need to reexamine national cybersquatting laws, such as the ACPA, to combat cryptosquatting explicitly and adequately. Moreover, creating a global UDRP-like system for resolving disputes involving BDNs (e.g., the proposed UBDRP) could be beneficial. Combined with other industry-specific

---

320 *See id.* (stating that "As highlighted by Tapscott, 'The blockchain movement is overpopulated by men' (Tapscott and Tapscott 2018, 287). Our qualitative analysis lacked representation from female subject matter experts. Therefore, it is crucial that future studies and policy development initiatives prioritise and ensure balanced participation of both male and female stakeholders. By doing so, we can harness a diverse range of perspectives, experiences, and insights, enabling the creation of more inclusive and effective policies that address the needs and concerns of all individuals involved in the Blockchain and DNS ecosystem.").

321 Catherine Mateu et al., *White Paper Trademarks in the Metaverse,* Int'l Trademark Ass'n (Apr. 2023), https://www.inta.org/wp-content/uploads/public-files/perspectives/industry-research/METAVERSE_REPORT-070323.pdf.

measures, the proposed solutions described above would help ensure that trademark owners can protect their rights in the new Web 3.0 environment.