INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE NEXUS OF TRADEMARKS AND DOMAIN NAMES: A LEGAL AND STRATEGIC ANALYSIS FOR BRAND OWNERS

AUTHOR - SHWETA ANAND, STUDENT AT AMITY LAW SCHOOL, PATNA

BEST CITATION - SHWETA ANAND, THE NEXUS OF TRADEMARKS AND DOMAIN NAMES: A LEGAL AND STRATEGIC ANALYSIS FOR BRAND OWNERS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (13) OF 2025, PG. 118-129, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

This paper addresses the fundamental conflict inherent at the nexus of trademark law and the Domain Name System (DNS), analyzing how the "first-come, first-served" technical nature of domain registration inherently clashes with intellectual property rights based on source identification and use in commerce. The resultant friction point—largely manifested through cybersquatting and its variations—necessitated the development of specialized enforcement architectures. The investigation provides an expert strategic analysis of the two dominant, yet distinct, dispute resolution avenues available to brand owners: the global, administrative Uniform Domain-Name Dispute Resolution Policy (UDRP) and the national, judicial Anti cyber squatting Consumer Protection Act (ACPA). The study demonstrates that effective brand protection necessitates a coordinated, multi-jurisdictional approach, strategically leveraging the speed of the UDRP for rapid domain recovery and the deterrence power of the ACPA for statutory damages and comprehensive injunctive relief. Finally, the paper assesses emerging strategic threats, particularly the increasing administrative complexity imposed by new generic Top-Level Domains (gTLDs) and the critical governance vacuum created by decentralized Blockchain Domain Name Systems (BDNS) , offering crucial foresight for future brand defense strategies.

Background: The Conceptual Dissonance Between Trademarks and Domains

1. The Functional Distinction and Inevitable Conflict

The regulatory framework governing intellectual property (IP) rights and the technical infrastructure managing global internet addresses originate from distinct, incompatible premises, generating a continuous structural tension that defines modern online brand enforcement. The core purpose of a trademark is to identify the source of goods or services, enabling consumers to distinguish offerings from one enterprise from those of another, as exemplified by choosing between a COKE® and a PEPSI®.[2] Trademark rights are established either through actual use in commerce, which generates common law rights in relevant geographic areas, or through formal registration based on existing or intended use.[2] This system fundamentally relies on consumer association and the distinctiveness of the mark.

In direct contrast, the Domain Name System (DNS) was initially designed purely as a technical scheme to simplify network navigation by translating complex Internet Protocol (IP) addresses into easily memorable text strings.[9] Domain registration, governed by registrars under the oversight of the Internet Corporation for Assigned Names and Numbers (ICANN), operates on a pragmatic "first-come, first-served" basis.[1] This principle means that technical registration occurs independent of

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

any substantive consideration for pre-existing IP rights.[1]

The inevitable conflict arises because domain names have undergone a functional transmutation, evolving from mere technical locators into critical business identifiers.[9] The Uniform Resource Locator (URL) frequently serves the commercial function of a trademark—identifying the source of online goods or services. When a third party registers a domain identical or confusingly similar to a protected mark, the technical identifier directly clashes with the legal system of source identification.[9] This inherent structural flaw—where a low-cost, global registration system lacks mandatory pre-screening for established IP [9]—makes cybersquatting a simple and low-risk activity for malicious actors, compelling legitimate brand owners to engage in expensive reactive enforcement measures.[8]

2. Defining Cybersquatting and Typosquatting

The primary manifestation of the trademark-domain name conflict is **cybersquatting**. This practice involves the pre-emptive, bad-faith registration of trademarks, famous personal names, or established business identifiers as domain names by third parties lacking any legitimate connection to the brand.[9] Cybersquatters exploit the simplicity of registration to hoard names, often with the explicit intention of offering them for sale to the legitimate company or person involved at prices far exceeding the cost of registration.[9] Alternatively, they may use the domains to divert internet traffic toward their own commercial sites, thereby exploiting the goodwill associated with the protected mark.[9]

A particularly pernicious subset of abusive registration is **typosquatting**. This involves registering domain names that utilize common misspellings, omissions, additions, or substitutions of letters within a well-known trademark.[11] For instance, registering a domain such as hyperlonmt.com for a mark like HYPERLOMNT [12] or bzzaget.com by omitting the letter 't' from BZZAGENT.[11] The objective is consumer confusion, capitalizing on common typographical errors to divert traffic intended for the legitimate brand owner.[4] This diverted traffic is often channeled to pay-per-click (PPC) parking pages or dubious, changing websites, which serves as clear evidence of the requisite bad faith for dispute resolution purposes.[12]

This continuous structural friction results from disjointed governance. Trademark rights are secured through territorial, resource-intensive national processes and standardized internationally through treaties like the Paris Convention and the Madrid Protocol.[8] Conversely, domain registration is cheap, immediate, and global. The lack of mandatory pre-screening at the registrar level, the administrative gap in the DNS ecosystem, allows the easily acquired technical identifier to override pre-existing, legally protected IP rights. This systemic failure forces international bodies like ICANN and WIPO to establish reactive, post-hoc dispute resolution procedures, such as the UDRP, as a necessary measure to correct the DNS's inherent inability to safeguard IP upon registration.[9]

International and National Regulatory Architecture

Effective defence of brand integrity requires navigating a complex, tiered regulatory architecture that includes global policy-setting and specific national statutory enforcement mechanisms.

1. The Global Governance Role of ICANN and WIPO

The governance of the global DNS relies heavily on the collaboration between ICANN, the technical coordinator, and WIPO, the global IP authority.

The **Internet Corporation for Assigned Names and Numbers (ICANN)** is the centralized private non-profit organization responsible for setting the policy for the Domain Name System, including the administration of generic Top-Level Domains (gTLDs).[14] ICANN's mandate to maintain a stable and secure DNS led directly to

its adoption of the UDRP to mitigate the escalating legal conflicts.[15]

The **World Intellectual Property Organization (WIPO)** is a treaty-based organization, supported by 171 Member States, dedicated to promoting the protection and use of intellectual property worldwide.[16] WIPO's services include providing a forum for international IP policy development and administering systems that allow for multinational protection of patents, trademarks, and industrial designs. Crucially, WIPO developed the UDRP and its Arbitration and Mediation Center became the first accredited UDRP service provider in 1999.[15]

These operational enforcement structures are framed by key multilateral IP treaties. The **Paris Convention for the Protection of Industrial Property** and the **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)** both contain provisions recognizing and protecting famous and well-known marks.[13] Although the TRIPS Agreement came into force prior to the full domain name crisis, its provisions are broadly interpreted to cover domain names, particularly given their function as "digital trademarks" in the contemporary commercial space.[19] Treaties such as the **Trademark Law Treaty (TLT)** and the **Madrid Protocol** further simplify and harmonize the procedures for obtaining and administering trademark protection across numerous countries.[13]

2. Foundational National Statutory Frameworks

In the United States, the core national legislation governing IP in digital media is the **Lanham Act** (Trademark Act of 1946).[21] The Lanham Act establishes the system for trademark registration and protects mark owners against the unauthorized use of similar marks that could result in consumer confusion.[21] This legislation provides the legal foundation for all domestic trademark infringement and dilution claims, including those involving domain names.

A key recent development augmenting the national framework is the **Trademark Modernization Act (TMA) of 2020**.[22] The TMA introduced efficient tools designed to clear the federal trademark register of unused marks, ensuring greater accuracy and integrity. Specifically, it created two new *ex parte* cancellation proceedings—expungement and re examination—that allow parties to challenge registered goods or services for non use in commerce.[22] This focus on eliminating "deadwood" through a faster and less expensive administrative alternative indirectly strengthens brand portfolios by clarifying the scope of existing rights, which is vital when assessing conflicts with domain name registrations.

3. Enforcement Against Infringing Content

While the UDRP focuses solely on the domain name itself, national legal systems must address liability for infringing content hosted on websites. European jurisprudence, for example, has assessed intermediary liability in depth. The CJEU has examined the balance between fundamental rights and IP enforcement in the context of website blocking, determining that service providers must generally bear the cost of necessary blocking measures.[23] Furthermore, Italian courts have, in exceptional circumstances, considered registry liability for aiding and abetting trademark infringements where the applicant's unauthorized use was deemed obvious.[23]

Separately, the **Digital Millennium Copyright Act (DMCA)** of 1998, while primarily a cornerstone of copyright protection, set essential precedents for digital IP enforcement.[21] It requires member states to adopt legislation preventing the circumvention of technical measures used to protect digital content and prohibits the removal of copyright management information.[24] Although not directly addressing trademark issues, the DMCA's framework established standards for online liability and enforcement that inform how courts approach IP protection in the digital sphere generally.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The UDRP: An Expedited Global Enforcement Mechanism

The UDRP is a binding legal framework established by ICANN and WIPO specifically to resolve disputes arising from the abusive registration and use of domain names in gTLDs and participating country code Top-Level Domains (ccTLDs).[15]

1. Policy Scope and Procedural Advantages

The UDRP is a **consensus policy** [17], meaning adherence is mandatory for all ICANN-accredited registrars, and any person registering a domain in these TLDs consents to its terms.[15] It is designed explicitly for classic cases of cybersquatting and abusive registration where trademark rights are clearly violated.[26]

The procedural benefits of the UDRP are its speed, low cost, and global reach. Proceedings are administrative, not judicial, typically concluding in less than two months, which is significantly shorter and cheaper than national litigation.[28] Furthermore, the UDRP applies worldwide, making it an effective tool against foreign cyber squatters without complex jurisdictional requirements.[29] WIPO's Arbitration and Mediation Center is the leading global provider of these dispute resolution services.[15]

Crucially, the UDRP offers only limited remedies: the **transfer** or **cancellation** of the disputed domain name.[4] It does not provide for monetary damages, statutory fines, or legal fee recovery.[4] This deliberate limitation defines the policy's role as a rapid administrative tool for regaining domain control, prioritizing the restoration of online identity over full financial redress.

2. The Three Mandatory Elements for Success

A complainant must successfully prove all three cumulative requirements outlined in Paragraph 4(a) of the UDRP Policy [15]:

- **Identity or Confusing Similarity (Element I)**

The complainant must establish that the domain name is identical or confusingly similar to a trademark or service mark in which the complainant holds rights.[15] These rights can be derived from formal registration or, critically, from unregistered

common law rights.[15] To establish common law rights under the UDRP, the complainant must demonstrate that the mark has acquired secondary meaning—a distinctive identifier which consumers associate exclusively with the complainant's goods or services.[32] Proof of secondary meaning involves showing the duration and nature of use, the volume of sales, and the extent of advertising under the mark.[32]

- **Lack of Rights or Legitimate Interests (Element II)**

The complainant must make a *prima facie* case that the respondent lacks any rights or legitimate interests in the domain name, upon which the burden of demonstrating such legitimacy shifts to the respondent.[33]

Legitimate interests can include: demonstrable preparations for *bona fide* use of the domain name in connection with a legitimate offering; being commonly known by the name independently of the domain registration (e.g., corporate name or nickname) [32]; or legitimate fair use.

For resellers or distributors claiming legitimate interest through **nominative fair use**, panels apply the rigorous **"Oki Data test,"** requiring four cumulative criteria: (1) the respondent must actually offer the trademarked goods or services; (2) the site must sell *only* the trademarked goods or services; (3) the site must accurately and prominently disclose the registrant's non-affiliation with the trademark holder; and (4) the respondent must not be attempting to "corner the market" in the trademarked domain names.[33] Conversely, criticism sites using a trademark plus a derogatory term (e.g., <trademarksucks.tld>) may establish legitimate interest if the use is genuinely noncommercial and non-misleading; however, identical domains used for criticism generally fail this test due to the high risk of impersonation.[33]

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

3. Bad Faith Registration and Use

The complainant must prove that the domain name was registered and is being used in bad faith.[15] The dual requirement means that mere renewal of an existing domain registration is generally insufficient to prove bad faith *registration* if the original registration was in good faith.[35]

Indicators of Bad Faith: Evidence reviewed by panels includes registering multiple trademark-similar domain names; using the domain to disrupt a competitor's business; the specific practice of typo squatting [1]; or offering to sell the domain name to the trademark owner for profit exceeding documented costs.[1]

The Passive Holding Doctrine: A critical consensus view under WIPO Overview 3.0, Section 3.3, confirms that bad faith "use" does not necessarily require an active use.[33] The **passive holding** of a domain name, especially one incorporating a famous mark, can constitute bad faith *use* under the Policy, preventing cyber squatters from simply registering a valuable mark and lying dormant to avoid enforcement.[38]

Privacy Services: While legitimate, the use of privacy or proxy services may support an inference of bad faith if the panel concludes the service is being used primarily to mask the underlying registrant's identity or the timing of the domain acquisition to avoid UDRP notification.[33]

The high rate of success for complainants in UDRP proceedings (over 90% in WIPO cases) [29] demonstrates its efficacy as a dedicated tool for correcting the DNS's tendency toward abusive registrations.[27] The limited remedy of transfer ensures that the process remains streamlined, bypassing the protracted, costly, and complex jurisdictional issues that accompany traditional IP litigation.[5]

The ACPA vs. UDRP: Strategic Choice and Complementary Remedies

For brand owners seeking enforcement against domain abuse, the selection between the administrative UDRP process and litigation under the U.S. Anti cybersquatting Consumer Protection Act (ACPA) is a crucial strategic decision based on the location of the parties and the ultimate enforcement goal.

1. Legislative Intent and Jurisdictional Scope

The **ACPA**, enacted as an amendment to the Lanham Act in 1999, is a specific U.S. federal remedy designed to target and deter cybersquatting within the United States.[3] Unlike the globally applicable UDRP [29], the ACPA is limited to U.S. federal courts.[40]

A paramount advantage of the ACPA is its provision for **in rem** jurisdiction.[5] This allows the trademark owner to initiate an action against the domain name itself, even if the registrant is outside the court's personal jurisdiction or cannot be located, provided the domain is held by a U.S.-based registrar.[5] This capability is unavailable under the UDRP.[15] Furthermore, the ACPA explicitly protects personal names against abuse, regardless of whether the individual has developed formal service mark rights, a scope broader than the UDRP.[5]

2. Differences in Legal Standards and Evidentiary Burden

The core distinction between the two systems lies in the burden of proof regarding malicious intent.

The **ACPA** requires the plaintiff to prove that the defendant had a specific **bad faith intent to profit** from registering, using, or trafficking in the domain name.[40] The statute provides several factors courts consider when assessing this intent. The similarity standard under the ACPA ("confusingly similar") is generally easier to meet than the "likelihood of confusion" standard required for traditional trademark infringement claims.[5]

In contrast, the **UDRP** requires proving bad faith *registration* and *use*.[35] While the ACPA focuses on subjective commercial motive, the UDRP focuses on objective abusive conduct. Complex cases involving competing rights, circumstantial evidence of intent, or extensive

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

testimony are generally better suited for the federal courts utilizing the ACPA than for the expedited administrative panels of the UDRP.[5]

3. Comparative Remedies: Deterrence vs. Possession

The selection of venue is ultimately driven by the desired remedy. The following table summarizes the key differences:

Comparative Analysis of Domain Name Dispute Resolution Avenues

Feature	UDRP Administrative Proceeding	ACPA (U.S. Federal Court Action)
Governing Authority	ICANN/WIPO Dispute Panels	U.S. Federal Courts
Jurisdictional Scope	Global (gTLDs and participating ccTLDs)	Confined to United States
Legal Burden	Bad faith *registration* and *use*	Bad faith *intent to profit*
Procedural Efficiency	Fast (typically days), low cost	Slow, expensive, full litigation process
Remedies Available	Domain Name Transfer or Cancellation only	Transfer, Cancellation, Injunctive Relief, and Statutory Damages (up to $100,000 per domain)
In Rem Action	Not available	Available (action against the domain name itself)

The most significant strategic difference is the availability of monetary relief under the ACPA. A successful ACPA plaintiff can obtain statutory damages ranging from $1,000 up to $100,000 per domain, alongside injunctive relief to immediately halt misuse.[4] These damages are a powerful deterrent, transforming the cost-benefit analysis for professional cyber squatters. While a UDRP loss merely results in the transfer of the domain, an ACPA judgment carries the potential for massive financial ruin. Therefore, the strategic value of the ACPA lies not just in recovering the domain but in providing a potent tool for dissuading future habitual abuse, a function the administrative UDRP cannot fulfill.

Observation: Proactive Domain Portfolio Defense Strategy

1. Strategic Domain Portfolio Management

Given the low barrier to entry for cybersquatting, brand protection requires a comprehensive and continuous strategic approach to domain portfolio management. Brands must move beyond simply securing their primary domain. Strategic planning involves the acquisition and

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 13 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

maintenance of multiple domain assets aligned with the overall brand architecture.

Defensive registration is fundamental risk mitigation. Recognizing that owning a trademark does not automatically grant ownership of the corresponding domain name necessitates explicit defensive action. This action includes securing common misspellings (anti-typo squatting), acquiring key variations across major gTLDs (e.g.,.net, .org), and registering product-specific or relevant geographic domains. This comprehensive defence maintains control over the brand's online identity and shields the brand image from confusion and misrepresentation by competitors or malicious entities.

2. Navigating the New gTLD Landscape

The proliferation of thousands of new generic Top-Level Domains (gTLDs) has simultaneously expanded opportunities for digital branding and vastly increased the surface area for trademark infringement.[42] This expansion imposes a significant administrative burden, requiring trademark holders to expend greater time and resources monitoring these new extensions.

The **Trademark Clearinghouse (TMCH)** is the essential ICANN-mandated defensive mechanism for managing this risk. The TMCH verifies registered marks, granting brand owners priority access during the **Sunrise Phase**—the initial launch period of any new gTLD. This priority access is vital for securing matching domains and proactively preventing fraud. Following the Sunrise Phase, the TMCH operates a

Claims Period, which notifies brand owners if a third party attempts to register a domain matching their verified mark, allowing for immediate intervention. For large entities, acquiring a proprietary **.BRAND gTLD** offers the highest level of control and security. Domains used singularly by the brand (e.g., <product.brand>) enhance consumer trust, mitigate phishing risks, and ensure complete control over the digital environment.

The growing number of TLDs transforms trademark monitoring from a legal task into a continuous, high-volume operational imperative. Since universal defensive registration is impractical, the effective strategy relies on leveraging the centralized administrative framework of the TMCH to automate early warning and priority registration. This requires legal teams to integrate advanced technical monitoring solutions and dedicate financial resources to proactive defence, rather than waiting for damage to accrue and necessitate expensive, reactive litigation.

3. Continuous Monitoring and Enforcement

A robust defence strategy mandates continuous vigilance across the digital threat landscape. Given that the volume of gTLDs and ccTLDs exceeds 2,000, specialized domain monitoring services are necessary to continuously analyse passive DNS data, SSL certificate logs, and zone files. This proactive collection of domain data provides broad visibility into the threat landscape, speeding up detection far beyond what traditional search engine monitoring can achieve. Continuous monitoring provides timely, actionable alerts regarding suspicious domains, allowing brands to limit the damage caused by infringement, counterfeit operations, and targeted phishing attempts.

Way Forward: Navigating Decentralization and the Web3 Threat

1. The Emergence of Blockchain Domain Names (BDNS)

The rise of decentralized naming systems represents the next critical challenge to global IP governance. **Blockchain Domain Name Systems (BDNS)**, such as the Ethereum Name Service (ENS) using the .eth extension or Unstoppable Domains, operate on decentralized ledgers secured by smart contracts. These systems function entirely outside the traditional, centralized ICANN/DNS framework and are technologically

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 13 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

incompatible with it. BDNS link human-readable names to specific blockchain wallet addresses, serving as multipurpose identifiers for Web3 applications and crypto assets.[7] The market for these domains is substantial and continuously growing, with millions of BDNs purchased or minted.[7]

2. Legal Challenges Posed by Decentralization

BDNS currently presents a significant challenge to brand integrity because its decentralized structure creates a fundamental **regulatory vacuum**. BDNS platforms allow the registration of names identical or similar to well-known trademarks (e.g., celine.nft) because they lack centralized oversight and do not implement trademark clearance procedures.

The most severe consequence of this architecture is the effective **failure of UDRP jurisdiction**. The UDRP relies entirely on a centralized registrar to execute the panel's order for domain transfer or cancellation.[25] Since BDNS systems operate on decentralized smart contracts without a central authority that can be compelled to act, the UDRP mechanism is rendered non-functional in this space.[14]

Furthermore, the decentralized and often pseudo-anonymous nature of BDNS registrants complicates traditional litigation. Proving personal jurisdiction or executing *in rem* actions (like those available under the ACPA) against assets held on a distributed ledger is extremely difficult.[7] This jurisdictional dead zone undermines both the speed of administrative enforcement and the deterrence of national statutory damages. The unregulated nature of BDNS increases the risk of abusive activity and mistrust in the system.[6]

3. Policy Recommendations and Strategic Adaptation

The challenges posed by BDNS require brand owners to shift their focus from reactive legal enforcement to proactive technical and governance engagement.

1. **Multi-Stakeholder Governance:** Policy adaptation must involve fostering multi-stakeholder alliances (such as the Web3 Domain Alliance) to discuss and develop shared governance frameworks for BDNS.[6] Even if this moves the system away from absolute decentralization, coordinated governance is necessary to create a "healthier" environment and address brand infringement.
2. **Blacklisting Mechanisms:** Brand owners must lobby for the implementation of technical "blacklist" systems within major BDNS providers (e.g., ENS Labs) to prevent the abusive registration of well-known marks at the source, addressing name collisions and infringement proactively.
3. **Defensive Acquisition (Web3):** As an immediate, necessary defense, brand owners must defensively acquire their key marks across all major BDNS extensions (e.g., .eth, .nft).[7] This defensive acquisition strategy, mirroring early internet practice, is the only current reliable method to prevent the confusion and abuse stemming from the fundamental absence of effective centralized enforcement.

Conclusion

The nexus between trademarks and domain names constitutes a perpetually contested arena defined by the clash between established IP legal principles and the dynamic, first-come, first-served mechanism of the global addressing system. Brand owners must operate under the recognition that this structural conflict necessitates continuous, layered, and proactive defense.

Strategic success hinges on three critical pillars: the integration of existing enforcement tools, meticulous proactive portfolio management, and foresight regarding emerging decentralized threats.

First, **integrated enforcement** requires utilizing the UDRP for rapid, cost-effective global domain recovery—acting as the essential triage

mechanism for abusive registration. This administrative speed must be strategically complemented by the ACPA, which provides the critical power of deterrence through statutory damages and the capability of *in rem* action against elusive cyber squatters in the U.S.

Second, **proactive portfolio management** is paramount. The proliferation of gTLDs demands that defensive registration strategies are centralized, leveraging the Trademark Clearinghouse to efficiently manage registration windows and monitor infringement risks across the vast domain landscape.

Third, **future policy adaptation** must address the acute governance crisis posed by decentralized Blockchain Domain Name Systems (BDNS). Because BDNS architecture currently nullifies the jurisdiction of the UDRP and complicates traditional litigation, brand strategy must immediately incorporate defensive registration in Web3 ecosystems and actively support multi-stakeholder initiatives aimed at implementing technical enforcement solutions, such as internal blacklisting, to safeguard brand trust in the future decentralized internet.

Only through this agile, coordinated, and technologically informed strategic approach can brand owners effectively maintain integrity and control over their digital identities in a globally interconnected environment defined by constant innovation and structural risk.

Works cited / References :

1. Trademark Use and Trademark Infringement in Domain Names - Dunlap Bennett & Ludwig, accessed October 2, 2025, https://www.dbllawyers.com/trademark-use-and-domain-names/
2. Trademark Fundamentals - Trademarks and Licensing Services, accessed October 2, 2025, https://trademarks.usc.edu/trademark-fundamentals/
3. THE UDRP AND THE ACPA: WHAT ARE THEY, AND WHICH SHOULD BE USED? | The Manitoba Law Journal, accessed October 2, 2025, https://themanitobalawjournal.com/wp-content/uploads/articles/MLJ_28.4/The-UDRP-and-the-ACPA-What-Are-They-and-Which-Should-Be-Used.pdf
4. Anti-cybersquatting Consumer Protection Act vs. UDRP - Revision Legal, accessed October 2, 2025, https://revisionlegal.com/internet-law/cybersquatting-lawyer/anti-cybersquatting-consumer-protection-act-vs-udrp/
5. UDRP Versus ACPA: Choosing the Right Tool to Challenge Cybersquatting - Fenwick, accessed October 2, 2025, https://assets.fenwick.com/legacy/FenwickDocuments/UDRP_Versus_ACPA.pdf
6. Full article: Web 3 disruption and the domain name system: understanding the trends of blockchain domain names and the policy implications, accessed October 2, 2025, https://www.tandfonline.com/doi/full/10.1080/23738871.2023.2294759
7. Global Brand Protection in Web 3.0: Blockchain Domain Names and New Legal Challenges - LARC @ Cardozo Law, accessed October 2, 2025, https://larc.cardozo.yu.edu/cgi/viewcontent.cgi?article=1098&context=ciclr-online
8. PROFESSIONAL POINTER: Domain Name Strategy to Protect Brand Identity, accessed October 2, 2025, https://bpp.msu.edu/magazine/domain-name-strategy-to-protect-brand-identity-september2020/
9. Frequently Asked Questions: Internet Domain Names - WIPO, accessed October 2, 2025, https://www.wipo.int/amc/en/center/faq/domains.html

10. The Interplay between Domain Names and Trademarks - Berry Moorman, accessed October 2, 2025, https://berrymoorman.com/the-interplay-between-domain-names-and-trademarks/
11. Full Text Search on WIPO Panel Decisions, accessed October 2, 2025, https://www.wipo.int/amc/en/domains/search/fulltext_decisions.jsp?q=typosquatting&start=3760
12. Full Text Search on WIPO Panel Decisions, accessed October 2, 2025, https://www.wipo.int/amc/en/domains/search/fulltext_decisions.jsp?q=typosquatting
13. International IP treaties | USPTO, accessed October 2, 2025, https://www.uspto.gov/ip-policy/international-ip-treaties
14. Trademarks on the Blockchain: NFT Domains and Collisions - University of Michigan Law School Scholarship Repository, accessed October 2, 2025, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1062&context=mtlr
15. WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP), accessed October 2, 2025, https://www.wipo.int/amc/en/domains/guide/
16. WIPO Internet Domain Name Process, accessed October 2, 2025, https://www.wipo.int/amc/en/processes/process1/report/finalreport.html
17. Tackling bad faith registration of domain names in a fast-changing landscape - WIPO, accessed October 2, 2025, https://www.wipo.int/web/wipo-magazine/articles/tackling-bad-faith-registration-of-domain-names-in-a-fast-changing-landscape-41179
18. WIPO Internet Domain Name Process, accessed October 2, 2025, https://www.wipo.int/amc/en/processes/process1/rfc/3/interim2_ch4.html
19. DOMAIN NAMES & (TRIPS): THE ASPECT OF PROTECTIONS ROOTS - SEA Open Research, accessed October 2, 2025, https://seaopenresearch.eu/Journals/articles/LSO_9_1.pdf
20. Trademark Law Treaty (TLT) - WIPO, accessed October 2, 2025, https://www.wipo.int/treaties/en/ip/tlt/
21. How Federal Laws Protect Intellectual Property in Digital Media - Leppard Law, accessed October 2, 2025, https://federal-criminal.com/white-collar/how-federal-laws-protect-intellectual-property-in-digital-media/
22. USPTO implements the Trademark Modernization Act, accessed October 2, 2025, https://www.uspto.gov/trademarks/laws/2020-modernization-act
23. The Role of the Domain Name System and Its Operators in Online Copyright Enforcement - WIPO, accessed October 2, 2025, https://www.wipo.int/documents/2810628/2827506/case-study-the-role-of-dns-and-operators.pdf
24. The Digital Millennium Copyright Act Enters a New Era | Penn Libraries, accessed October 2, 2025, https://www.library.upenn.edu/news/dmca-update
25. Uniform Domain-Name Dispute-Resolution Policy - icann, accessed October 2, 2025, https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en
26. UDRP Procedure Explained - BrandShelter™, accessed October 2, 2025,

https://www.brandshelter.com/glossary/udrp-procedure/

27. Judicial Review of ICANN Domain Name Dispute Decisions - Santa Clara Law Digital Commons, accessed October 2, 2025, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1293&context=chtlj
28. In a nutshell: The WIPO UDRP for domain name disputes - Novagraaf, accessed October 2, 2025, https://www.novagraaf.com/en/insights/nutshell-wipo-udrp-domain-name-disputes
29. Cyber Center: The Continued Hijacking and Ransoming of the Domain Name System by Modern-Day Corporate Privateers - American Bar Association, accessed October 2, 2025, https://www.americanbar.org/groups/business_law/resources/business-law-today/2016-june/cyber-center-the-continued-hijacking-and-ransoming/
30. A Second Bite at the Apple: Domain Name Registrants Can Use Anticybersquatting Statute to Reverse UDRP Proceeding - WilmerHale, accessed October 2, 2025, https://www.wilmerhale.com/en/insights/publications/a-second-bite-at-the-apple-domain-name-registrants-can-use-anticybersquatting-statute-to-reverse-udrp-proceeding-february-13-2002
31. Uniform Domain-Name Dispute-Resolution Policy - Wikipedia, accessed October 2, 2025, https://en.wikipedia.org/wiki/Uniform_Domain-Name_Dispute-Resolution_Policy
32. WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition, ("WIPO Jurisprudential Overview 3.0"), accessed October 2, 2025, https://www.wipo.int/amc/en/domains/search/overview3.0/
33. WIPO Overview of WIPO Panel Views on Selected UDRP Questions ..., accessed October 2, 2025, https://www.wipo.int/amc/en/domains/search/overview3.0/#3
34. UDRP Division 4: Rights and Legitimate Interests - Full Text - Berkman Klein Center, accessed October 2, 2025, https://cyber.harvard.edu/udrp/opinion/itext.html
35. Bad Faith in UDRP domain name complaints - Taylor Wessing, accessed October 2, 2025, https://www.taylorwessing.com/en/insights-and-events/insights/2023/11/bu-bad-faith-in-udrp-domain-name-complaints
36. Licensees, Franchisees, Distributors & Resellers as Respondents in Domain Name UDRP Complaint Proceedings - JMB Davis Ben-David, accessed October 2, 2025, https://jmbdavis.com/knowledgebase/licensees-franchisees-distributors-resellers-as-respondents-in-domain-name-udrp-complaint-proceedings/
37. UDRP Proceedings | Internet, Domain Name, and Trademark Attorneys - Klemchuk, accessed October 2, 2025, https://www.klemchuk.com/udrp-proceedings
38. WIPO Domain Name Dispute Case No. D2024-4628, accessed October 2, 2025, https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2024-4628
39. What's Going on with the Passive Holding Doctrine? - vol 4.21 - InternetCommerce.org, accessed October 2, 2025, https://www.internetcommerce.org/udrp-case-summaries/whats-going-on-with-the-passive-holding-doctrine-vol-4-21/

40. The Anticybersquatting Consumer Protection Act and the Uniform Domain Name Dispute Resolution Policy The First Decade - Scholarly Commons @ UNLV Boyd Law, accessed October 2, 2025, https://scholars.law.unlv.edu/context/nlj/article/1181/viewcontent/nvj11_3_10_Scatturo.pdf

41. Domain Portfolio Management: Strategic Approaches for Multi-Brand Businesses, accessed October 2, 2025, https://www.ait.com/blog/domain-portfolio-management-strategic-approaches-for-multi-brand-businesses/?fbclid=IwAR2y6S9bOVJNRBxsTwf1Rka15faNh8Xgj5jjt_qrGMS2hfVRJ0DPkJnd58M&panel_id=19&utm_source=parked&utm_medium=redirect&utm_compaign=web-design

42. New gTLDs - EBRAND, accessed October 2, 2025, https://ebrand.com/new-gtlds/

43. I Cann't Believe It's Not Better: Why New gTLDs aer Bad for Brand Owners and Trademark Law, accessed October 2, 2025, https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1041&context=jipl