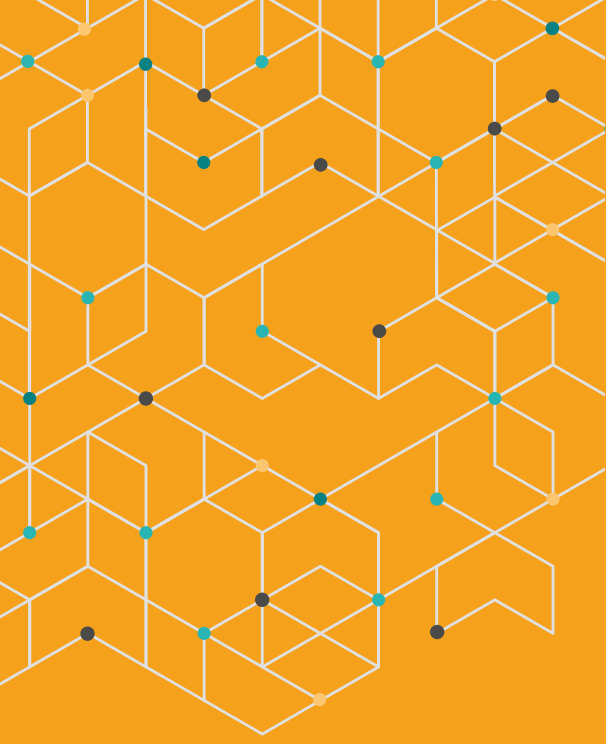
Resolution of Domain Name Conflicts: 15 Years of

SACI-Adm

registro.br nic.br cgi.br



Resolution of Domain Name Conflicts: 15 Years of SACI-Adm

registro.br nic.br cgi.br

This booklet is an appendix to the work "Resolução de conflitos de nomes de domínio: 15 anos de SACI-Adm (Resolution of Domain Name Conflicts: 15 Years of SACI-Adm)" and contains the original contributions, in English, by foreign authors invited to contribute to the book. The published collection includes translations into Portuguese, the language in which the rest of the texts are also available.

SACI-Adm

CREDITS

Production

NIC.br, CGI.br, and Registro.br

Executive coordination

Raquel Gatto

Organization

Pedro Lana and Maria Julya Oliveira

Graphic design and layout

Larissa Paschoal

2025

A Look Back into Alternative Dispute Resolution Mechanism for Domain Names and its Fundamentals of Success

Brian Beckham[1]
and Luisa Ferreira Gonzalez Penna[2]

Introduction

By the occasion of the 15-year anniversary of the SACI-Adm procedure, it is inevitable to look back into its predecessor, the Uniform Domain Name Dispute Resolution Policy (UDRP) to not only understand how the Brazilian mechanism came to be, but as well to identify the different elements that allowed such type of alternative dispute resolution mechanisms to be highly adopted and respected by different stakeholders, and each passing year, even more relevant to combat the increasing abusive conducts in the digital environment.

Established WIPO in 1999 following a robust international consultation process[3], and adopted by the Internet Corporation for Assigned Names and Numbers (ICANN), in response to the growing number of disputes over domain name registrations, the UDRP set the legal framework for countries around the world as to solving domain name disputes and its success

1 Head of the Internet Dispute Resolution Section at the World Intellectual Property Organization's Arbitration and Mediation Center, holds a J.D. and LL.M. in Information Technology from the John Marshall Law School in Chicago, Illinois. Brian is responsible for all aspects of the day-to-day management of WIPO's domain name services offered under the WIPO-initiated UDRP and related ccTLD policies. Brian also oversees WIPO's domain name-related policy activities, including representation at ICANN and industry meetings

2 Legal Case Manager at the World Intellectual Property Organization's Arbitration and Mediation Center.

3 Final Report of the First WIPO Internet Domain Name Process, April 30, 1999, available at https://www.wipo.int/amc/en/processes/process1/report/.

remains unquestionable 25 years later, with many countries having either adopted the UDRP as a mechanism, or variations thereof, as is the case of Brazil. Worth noting that, before the UDRP, there was no global framework to deal with cybersquatting and parties had mostly to rely on courts – if they could even do that, given that there were no national laws to deal with the new practice of cybersquatting – in order to tackle abusive registrations.

The novelty and quick developing nature of the Internet in the late 1990s represented a need for addressing bad faith domain name registrations. As disputes between trademark owners and domain registrants became more frequent, the need for a global, streamlined dispute resolution mechanism became urgent. However, even if national courts could deal with the emerging threat of cybersquatting, a court-based solution seemed inadequate to be effective in the global outreach of the Internet space as rightsholders would be forced to litigate in jurisdictions around the world. In this sense, the UDRP, by establishing design elements which allowed a fast, low-cost, and consistent process for resolving domain disputes outside traditional courts, quickly became the successful mechanism against cybersquatting.

The replication of the UDRP throughout countries around the world in the following years and until very recently is based on some fundamental elements that enabled the protection of trademarks in the Internet space and, as such, this article aims to analyze such fundamental elements of one of the most successful examples of alternative dispute resolution.

Combatting abusive registrations before the UDRP

To understand how dispute resolution policies, namely the UDRP came to be, it is important to understand the context that favored its creation. Prior to the UDRP, in the mid-1990s, the digital landscape was markedly different from the present days. At that time, the Internet resembled a "wild west" environment where there was no legal framework for addressing abusive conduct, and thus, no clear remedies for issues such as domain name infringement.

The dominant idea at that time, captured by influential works such John Perry Barlow's "Declaration of the Independence of Cyberspace[4] was that the cyberspace was beyond traditional legal jurisdiction, and a notable example of that scenario was in 1994, upon the registration of the <mcdonalds.com> domain name by journalist Joshua Quittner while

4 John Perry Barlow, A Declaration of the Independence of *Cyberspace* (1996), available at https://www.eff.org/cyberspace-independence.

conducting an experiment to illustrate the vulnerabilities in domain name registration at the time[5].

The registration of said domain name by the journalist, who was not affiliated with the fast-food giant, was intended to demonstrate a critical flaw in the Internet's regulatory framework, namely there was no framework to deal with registration by third parties of a brand owner's identity (and putting aside the first-come first-served and unverified nature of domain name registrations). After acquiring the domain, he contacted McDonald's Corporation and offered to hand over the domain in exchange for a donation to charity. The episode caused public and corporate alarm and became a landmark illustration of the so-called "wild west" era of the Internet—an unregulated space where intellectual property rights were not protected in digital contexts. The McDonald's case perfectly exemplified the legal vacuum surrounding cyberspace governance.

In this context of lack of legal remedies to combat these type of situation, trademark owners resorted to the main available measure at that time, that is, to file lawsuits on national courts under existing trademark or unfair competition laws, like the United States' Lanham Act to argue that the misuse of a domain name amounted to trademark infringement, or the Federal Trademark Dilution Act (FTDA), 15 U.S.C. § 1125(c) as well as under consumer rights legislation. In Brazil, trademark owners relied on Brazil's Industrial Property Law edited in 1996 (Lei 9.279/96), and on the Consumer Rights Protection Act (Lei 8.078/90)[6].

However, such national legal acts were not always adequate for the novel issues posed by domain names, leading to mixed results in court. In addition, litigation was jurisdictionally complicated, raising questions of personal jurisdiction, venue, and the applicability of national trademark law (grounded in "offline" physical sales of goods and services) to global online

5 Joshua Quittner, Billions Registered, Wired magazine (1994), available at https://www.wired.com/1994/10/mcdonalds/.

6 Some examples of domain name litigations from that time are Panavision Int'l, L.P. v. Toeppen (1998), in which a United States court ruled against a cybersquatter who had registered <panavision.com> and attempted to sell it back to the trademark owner. The court found that this behavior diluted the value of the trademark under the Federal Trademark Dilution Act. Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) This case became a landmark case defining cybersquatting as a form of unfair competition under United States law. In Brazil, some notorious cases are the disputes over the <globo.com.br> (1996) and <magazineluiza.com.br> (1998) domain names, decided based on Brazil's Industrial Property Law and unfair competition rules.

behavior. Other negative aspects were that litigation is often expensive and time-consuming, which contrasted with the fast pacing and ease nature of cybersquatting – which has virtually no barriers to entry (domain names cost only a few dollars compared to thousands required to go to court) and no penalties for repeat offenders.

As resorting to national courts represented a complicated and usually inadequate option, often companies chose to negotiate with domain name registrants and purchase the domain name from cybersquatters, often at extortionate and inflated prices, simply because such was faster and less costly solution compared to litigation. However, this practice quickly and unintentionally encouraged more cybersquatting, as it proved there was a market for selling trademarked domains.

As the issue of abusive registrations increased, some domain name registries or registrars (an industry that was just emerging at the time) opted for developing and implementing their own early dispute policies[7], but these varied widely in scope and effectiveness, being subject to criticism from both trademark owners and domain name registrants, and often did not result in an actual solution regarding ownership of the domain name [8].

The Creation of the UDRP

The UDRP was adopted by newly-established ICANN, in cooperation with WIPO, in a context of the proliferation of lawsuits targeting registrars and even the United States government, which played a fundamental role

7 An example of Registrar Policy from that time was is Network Solutions' Domain Name Dispute Policy created in 1995. The domain owner then had 30 days to show they had their own trademark rights or file a lawsuit.

8 Network Solutions' Domain Name Dispute Policy created in 1995 enabled the suspension of the domain name upon the simple submission of a trademark certificate, which some argued to represent a presumption of bad faith on the domain name registrant and a lack of due process. On the other hand, the remedy, which was limited to the suspension/on hold placement of the domain name was considered insufficient to solve the dispute and thus, rather than serving as an alternative solution to the courts, represented an increase in litigation. Marie-Emmanuelle HAAS, The origin of the UDRP: NSI's 1995 domain name dispute policy (2009) and Victoria Napolitano, Network Solutions 2000: The Internet Corporation for Assigned Names and Numbers' Uniform Domain Name Dispute Resolution Policy, 10 DePaul J. Art, Tech. & Intell. Prop. L. 537 (2000) Available at: https://via.library.depaul.edu/jatip/vol10/iss2/13.

in shaping the governance of the Internet, and a broader effort to transition the management of the Domain Name System from a government-administered system to a more private-sector-led, international "multistakeholder" model.

Prior to the creation of ICANN, the United States government, through the Department of Defense and later the National Science Foundation, had overseen key Internet functions, including the allocation of domain names and IP addresses. As the Internet rapidly expanded and commercial use became dominant in the 1990s, the need for a new governance model became apparent—one that could adapt to global participation while reducing direct government control[9].

In March 1994, Jon Postel published Request for Comments (RFC) 1591, titled *"Domain Name System Structure and Delegation"*[10], which became one of the foundational documents in Internet governance as it outlined the principles for the management and delegation of domain names within the Internet's Domain Name System, and more importantly, shifted the focus of the conversation regarding domain name management from an ownership perspective, to an approach more focused on use, responsibilities and the service to the Internet community, resulting in a service-based notion, rather than proprietary.

Later on, iIn February 1998, the United States Department of Commerce released the Green Paper, titled "A Proposal to Improve Technical Management of Internet Names and Addresses"[11]. This document outlined a preliminary plan for transferring the management of domain names and IP address allocation to a new private, non-profit organization. The Green Paper emphasized the need for competition, private sector leadership, and a transparent dispute resolution system. However, it drew criticism from various stakeholders, including international organizations and private sector actors, who argued against governmental control.

9 Mueller, Milton. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. MIT Press (2002).

10 RFC 1591 established the idea that that domain names are not property and should be analyzed as serving the interest of the broader Internet community. Domain holders, in that sense, were not seen as owners, but rather "trustees". https://www.rfc-editor.org/rfc/rfc1591.

11 U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA). A Proposal to Improve Technical Management of Internet Names and Addresses (Green Paper). January 30, 1998. https://www.ntia.doc.gov/files/ntia/publications/dnsdrft.txt

Responding to comments, the Department of Commerce issued a revised version—the White Paper—in June 1998, formally titled *"Management of Internet Names and Addresses"*[12]. The White Paper acknowledged the concerns raised in response to the Green Paper and proposed the formation of a new, internationally representative organization to manage these technical functions. The document emphasized four principles: stability, competition, private sector coordination, and representation. It also explicitly called for the creation of a new private entity—what would become ICANN—to carry out these responsibilities. By November 1998, ICANN was incorporated in California as a non-profit, and it began assuming responsibilities previously managed by the Internet Assigned Numbers Authority (IANA).

The Green and White Papers, along with RFC 1591, laid the groundwork for the creation of ICANN, which was established as a bottom-up consensus model to develop a universal, legally consistent response to domain name disputes. This new mechanism – the UDRP – introduced a concept akin to a modern Lex mercatoria, which allowed trademark holders to protect their rights online while maintaining the integrity and stability of the Domain Name System.

Early discussions in ICANN meetings highlighted the philosophical divide between the Internet as a space of idealistic freedom and the emerging reality of cybersquatting. While the Internet was initially viewed as a domain governed by principles of free information and "first come, first served," increasing abuse led to a backlash, exemplified by the McDonald's case already mentioned. Intellectual property advocates, such as the International Trademark Association (INTA), began forming committees to counter this growing threat, advocating for a system that could reconcile Internet freedom with the protection of intellectual property rights and ICANN resorted to the WIPO to study the issue and provide recommendations.

In 1998, WIPO launched the Internet Domain Name Process[13], engaging stakeholders from across the world to assess the legal and practical implications of domain name disputes. The resulting report, issued in April 1999, laid the foundation for what would become the UDRP. It

12 U.S. Department of Commerce, NTIA. Management of Internet Names and Addresses (White Paper). June 5, 1998. https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en.

13 Final Report of the WIPO Internet Domain Name Process of April 30, 1999 https://www.wipo.int/amc/en/processes/process1/report/finalreport.html.

recommended the creation of a uniform, non-judicial administrative procedure for resolving cases of bad-faith registration of domain names. ICANN adopted these recommendations almost in full, marking a landmark collaboration between international legal and Internet governance communities. WIPO was also designated as the first approved dispute resolution service provider, cementing its leading and ongoing role in the administration and stewardship of the UDRP.

Early years

The UDRP came into force on December 1, 1999, applying to all registrations under generic top-level domains (gTLDs). The submission to the procedure was mandatory and established by the domain name registration contract, a key element for the success of the procedure.

The early years of the UDRP were marked by a rapid adoption by trademark holders, who appreciated its relatively low cost, speed, and predictable outcomes compared to traditional litigation. Within the first three years of its implementation, WIPO had received over 3,000 of cases[14], demonstrating immediate and widespread acceptance of the mechanism. Its initial success not only mitigated the immediate harms of cybersquatting but also set enduring standards for efficient, fair, and accessible online dispute resolution.

The emerging idea of consistency of early decisions, particularly those rendered by experienced WIPO panelists, resulted in the creation of the WIPO Overview of WIPO Panel Views on Selected UDRP Questions[15], a compiled and systematized resource, enhanced predictability and transparency.

The experience from the early years also evidenced that the framework developed by the UDRP, although limited to addressing abusive domain name registrations, was not in itself restricted to the point to prevent interpretations, which in fact assisted the policy to, despite, unchanged, stay relevant more than 25 years later. In this regard, landmark cases such

14 https://www.wipo.int/amc/en/domains/statistics/domains.jsp

15 To this day, WIPO has edited three editions of the consensus view of panels on a range of common and important substantive and procedural issues, compiled in WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Original Edition (2005); WIPO Overview of WIPO Panel Views on Selected UDRP Questions, 2.0 (2011) and WIPO Overview of WIPO Panel Views on Selected UDRP Questions Overview 3.0 (2017).

as Telstra[16], which addressed passive domain holding, and Oki Data [17], which examined fair use, showcase the UDRP's ability to adapt to evolving Internet use cases. This adaptability has extended to impersonation and cases involving the use of new technologies, further demonstrating the policy's relevance.

Early empirical analyses revealed a strong success rate for complainants, often exceeding 80%, which reflected the policy's effectiveness in targeting clear cases of bad-faith registration and use. Notably, the UDRP also pioneered the broader field of online alternative dispute resolution (ADR), serving as a model for subsequent efforts in digital rights enforcement.

By 2005, the UDRP had firmly established itself as the leading mechanism for resolving domain name disputes globally, handling thousands of cases each year. Although there were occasional calls for reform mainly regarding procedural safeguards, ICANN chose to maintain the UDRP largely in its original form, citing its overall effectiveness. The UDRP's early and consistent success can be attributed to several key design elements. First, its procedural efficiency allowed disputes to be resolved within a matter of weeks, compared to the months or years often required in national courts. Second, the Policy's international scope addressed the jurisdictional challenges inherent in cross-border Internet disputes, providing a neutral forum where parties from different legal systems could seek redress. Third, the UDRP's relatively low costs democratized access to remedies, enabling not only large corporations but also small businesses and individual trademark holders to defend their rights online. These elements will be explored in further detail in the subsequent sections[18].

Design elements

Supranational, Uniform, and Global application

One of the most defining and innovative characteristics of the UDRP is its supranational, uniform, and global application. Unlike traditional

16 *Telstra Corporation Limited v. Nuclear Marshmallows*, WIPO Case No. D2000-0003.

17 *Oki Data Americas*, Inc. v. ASD, Inc., WIPO Case No. D2001-0903.

18 See generally The UDRP: Design Elements of an Effective Mechanism. Nicholas Smith and Erik Wilbers. The American Review of International Arbitration, December 2005.

legal mechanisms, which are confined within national borders and often complicated by questions of jurisdiction and applicable law, the UDRP was designed to operate independently of any single country's legal system.

As a condition of registering a domain name in a gTLD, registrants automatically agree to be bound by the UDRP, thereby consenting in advance to the procedures regardless of their geographic location. This supranational framework allows the UDRP to transcend national boundaries and complex legal systems, providing a singular, predictable regime for resolving domain name disputes worldwide. This uniform applicability, thus, removes the issue related to jurisdiction-like discussions as well as the issue of dealing with different legal systems depending on the location of the domain name registrant.

The UDRP's uniform application is another central aspect of its success. The Policy imposes the same substantive and procedural rules on all registrants and complainants, ensuring that disputes are adjudicated according to a consistent standard. This uniformity fosters predictability and legitimacy, allowing trademark owners and Internet users alike to rely on that disputes will not be subject to the divergent national trademark laws or judicial interpretations. It also streamlines the administration of disputes by accredited dispute resolution providers.

This uniform and supranational character of the UDRP was instrumental in securing its legitimacy and widespread acceptance among global stakeholders. By deliberately detaching the policy from national legal systems, the UDRP was perceived as a neutral and impartial mechanism, rather than as an extension of one state's legal or commercial interests[19]. This neutrality was particularly important in fostering trust among trademark holders, registrars, and domain name registrants—operating across different legal systems and contexts. Furthermore, the UDRP's universal applicability to all registrants of generic top-level domains, enforced through contractual obligations with registrars, underscored its legitimacy as a broadly consensual rather than coercive framework.[20]

Moreover, the UDRP's global reach reflects the borderless nature of the Internet itself. By creating a mechanism that is accessible to parties in any location, the UDRP addresses the fundamental challenge posed by the Internet's capacity to facilitate cross-border infringements without regard to physical or legal boundaries.

19 Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 Duke L.J. 187 (2000), at 198–201.

20 David R. Johnson & David Post, Governing Cyberspace, 48 Stan. L. Rev. 1367 (1996), at 1385

Safety Valve of appeal to Courts

Although criticism regarding the lack of an internal appeal procedure still exists when discussing potential improvements to the UDRP, the policy did maintain the option of parties resorting to court to resolve domain name related issues, including abusive domain name registrations. This design element is also present in the SACI-Adm procedure.

As explained above, even though the UDRP was conceived as a more efficient and adequate option than litigation, the UDRP was not intended to eliminate the parties' rights to initiate a lawsuit in a national court before, during, or after the conclusion of a UDRP proceeding.

This possibility of judicial recourse functions as an important safeguard against potential procedural unfairness or erroneous decisions by UDRP panels. It provides an external review mechanism that is independent of ICANN and the providers. Importantly, the judicial review is not constrained by the findings of the UDRP panel; rather, courts apply their own applicable law to the dispute and are empowered to reach different conclusions regarding ownership or use of the domain name. However, practical experience has shown that relatively few UDRP decisions are challenged in national courts. The generally high quality and consistency of panel decisions have meant that most parties accept the outcome of the administrative process and as such, is another testament to the success of the procedure.

The combination of a narrowly tailored administrative remedy — with procedural and substantive limitations, not encompassing an evidentiary phase that is typical of courts — with access to judicial oversight, reflects a careful balancing act between efficiency and fairness. The UDRP offers an expedited, cost-effective method to combat cybersquatting, in contrast to lengthy and costly discovery and motions practice in courts.

It should also be noted that although there is no formal "refiling" process within the UDRP, in some circumstances, parties have attempted to file new UDRP complaints involving the same domain name and parties, especially when new evidence or when changed circumstances arise. This practice is only permitted under limited

conditions by panels[21], typically where the second complaint is based on facts or legal theories not available at the time of the first decision. Thus, while the UDRP is fundamentally designed as a one-shot administrative system, in exceptional cases, re-filing opportunities, ensuring that the system remains both efficient and fair.

Low-cost and Standardized Payment

The low cost of UDRP proceedings, relative to traditional court litigation, is also a central reason for the policy's effectiveness and widespread acceptance. Court litigation over domain names often involves significant financial outlays, including filing fees, attorney's fees, expert witness costs, and potentially extensive discovery processes, particularly in cross-border disputes.

By contrast, UDRP proceedings are designed to be economical, with standardized filing fees and limited procedural steps. This cost-effectiveness makes it feasible for a broad range of trademark holders—including small businesses, non-profits, and individual entrepreneurs—to protect their rights online without prohibitive financial barriers. Furthermore, lower costs contribute to the speed and accessibility of the UDRP, reinforcing its function as a rapid remedy against cybersquatting that supports the stability and reliability of the domain name system.

The policy's structure places the initial burden of paying the dispute resolution service fees on the complainant. Considering the respondent is affected with the automatic submission to the UDRP per the registration agreements, and since it is the complainant who initiates the proceeding by the simple registration of a domain name, imposing the payment of the fees on the respondent in case of commencement of a dispute by complainant is not required.

Since the complainant seeks to alter the registrant's claim over a domain name, it is appropriate that the complainant bear the costs

21 Panels have accepted refiled complaints only in highly limited circumstances such as (i) when the complainant establishes that legally relevant developments have occurred since the original UDRP decision, (ii) a breach of natural justice or of due process has objectively occurred, (iii) where serious misconduct in the original case (such as perjured evidence) that influenced the outcome is subsequently identified, (iv) where new material evidence that was reasonably unavailable to the complainant during the original case is presented, or (v) where the case has previously been decided (including termination orders) expressly on a "without prejudice" basis. WIPO Overview 3.0, section 4. 18.

of triggering the process. Moreover, requiring complainants to pay discourages frivolous or speculative claims, ensuring that parties carefully assess the merits of their case before filing. Respondents are not financially burdened unless they elect to appoint a three-member panel rather than a single panelist—an option that is available to enhance perceived fairness where appropriate. This fee structure maintains access to justice for domain name holders, who may be individuals or small entities unfamiliar with legal procedures, while also preserving the overall legitimacy of the UDRP by promoting a balance between accessibility, deterrence of abuse, and procedural economy.

Rules for Language of Proceedings

Another element in the direction of fairness and in line with the intent of optimization of providing actual notice to the registrant of the domain name under a UDRP procedure is the rule establishing that the proceedings shall be conducted in the language of the registration agreement, which was used to register the domain name, unless otherwise agreed by the parties[22].

Considering again the pace of the UDRP proceedings, this provision respects the principle that registrants should be able to understand and respond to proceedings conducted in the language they encountered during the domain name registration process. However, the UDRP also affords panels a degree of flexibility: panels may decide to proceed in a different language where justice so requires, particularly in cases where one party would suffer prejudice due to language barriers or where the complainant can show that the respondent understands another language[23]. This flexibility serves to balance procedural fairness with practical considerations of efficiency and equity.

The choice of language has substantive implications for access to justice under the UDRP. If proceedings were routinely conducted in languages unfamiliar to respondents, it could undermine the legitimacy of the system by depriving them of a meaningful opportunity to defend their interests. Conversely, rigidly requiring proceedings to be conducted in all possible languages would represent an almost impossible task for the providers and would also significantly increase costs and delay, defeating the UDRP's core purpose of providing a cost-efficient dispute resolution mechanism. By allowing panels to weigh the facts of each case in determining the appropriate language,

22 UDRP Rules, paragraph 11.

23 WPO Overview 3.0, section 4.5.1.

the UDRP promotes procedural fairness while maintaining the overall efficiency that has been essential to its success.

No legal representation required

The UDRP is that it does not require parties to retain legal counsel in order to participate in proceedings. This aspect of the UDRP is critically important for ensuring that the dispute resolution process remains accessible, cost-effective, and efficient. As the UDRP was designed to address clear cases of abusive domain name registrations, intended to be simpler and less formal than traditional litigation, with also a clear and objective criteria for the granting of the remedy requested (transfer or cancellation, as further discussed below), requiring parties to retain counsel would increase the financial burden on both complainants and respondents, potentially discouraging legitimate claims or defenses, particularly among small businesses, non-profit organizations, and individual registrants who may lack the resources to engage specialized counsel.

By allowing parties to represent themselves, the UDRP democratizes access to justice within the domain name system, ensuring that remedies against abusive domain name registrations are not limited to large, well-resourced entities. Additionally, the UDRP's procedural rules, model pleadings, and publicly available case databases—such as WIPO's online resources—are designed to guide non-lawyers through the process effectively.

Importantly, the absence of a legal counsel requirement does not preclude parties from seeking professional assistance if they choose; it merely removes a to entry. This design choice reflects the UDRP's broader commitment to promoting an accessible, balanced, and globally usable system of dispute resolution, consistent with the decentralized and inclusive nature of the Internet itself.

Clear and objective criteria and examples

Another critical element to its success was the UDRP's substantive standard for adjudicating claims, which focused narrowly on cases of clear bad faith. Complainants were required to demonstrate three cumulative elements: (i) that the disputed domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; (ii) that the respondent has no rights or legitimate interests in respect of the domain name; and (iii) that the domain name has been registered and is being used in bad faith.

This carefully balanced test limited the scope of UDRP proceedings to straightforward cases of abuse, in principle avoiding complex factual or legal inquiries.

To assist panels and parties in interpreting these standards, Paragraph 4(b) of the UDRP provides a non-exhaustive list of examples that constitute evidence of bad faith, such as registering a domain name primarily to sell it to the trademark owner for profit, or using the domain to disrupt a competitor's business. Similarly, Paragraph 4(c) outlines defenses available to respondents, including being known by the domain name or preparations to start a business or demonstrating legitimate noncommercial or fair use of the domain name.

The importance of these clear criteria and illustrative examples, which are also similarly present in the SACI-Adm procedure, are fundamental, especially taking into account the above-cited non-requirement of parties to be represented by counsel. They serve to standardize decision-making and enhance predictability. By specifying uncontroversial grounds for establishing bad faith on the one hand or legitimate interests on the other, the UDRP reduces uncertainty for both complainants and respondents, enabling them to assess their positions more accurately before initiating or defending against a complaint. This transparency supports fairness and discourages frivolous or abusive filings, contributing to the UDRP's reputation as a balanced and reliable dispute resolution mechanism.

Moreover, the examples help streamline proceedings by providing panels with a structured framework for evaluating evidence, thereby facilitating efficient, consistent outcomes across thousands of disputes globally. Ultimately, the use of clear, objective criteria and practical examples, and, at the same time, by anchoring the analysis to established principles of trademark law, reflects the UDRP's broader goal of creating a uniform, accessible, and principled system of domain name dispute resolution.

Single round of pleadings and Timelines

Once again within the notion of the conception of the UDRP as a quick and efficient procedure to fight bad faith registrations, the policy provides only for a single round of pleadings. Even though supplemental filings may be accepted on panel's discretion, such are considered on an exceptional basis.

The limitation regarding the moment for the pleadings promotes procedural economy by focusing the parties' arguments early and minimizing the risk of prolonged, adversarial litigation that could otherwise undermine the procedure's efficiency goals. Furthermore,

the policy imposes strict deadlines at each stage. The importance of these streamlined procedures lies in their ability to deliver swift outcomes, which is critical in domain name disputes where delay can cause ongoing commercial harm or facilitate the use of domain names to perpetrate illegal activities such as fraud.

Specified and Limited Remedies

The only remedies available under UDRP proceedings are either the transfer of cancellation of a domain name, without the possibility of any type of injunction or compensation requests. This limited remedial prevents the administrative system from becoming a substitute for comprehensive litigation and ensures that complex claims requiring extensive factual investigation, such as damages assessments, remain within the purview of courts.

The emphasis on specified remedies also minimizes the stakes of the administrative procedure, which encourages parties to participate without fear of disproportionate financial or legal exposure. It focuses the proceedings solely on the abusive aspect of registration and use of the domain names, aligning with the UDRP's purpose of addressing abusive conduct rather than adjudicating broader commercial disputes.

Online communications

Given the inherently global and digital nature of the Internet, an effective dispute resolution system must transcend national borders and traditional courtroom procedures. Conducting Internet dispute proceedings online ensures that parties located in different countries can participate equally without facing prohibitive logistical or financial barriers associated with in-person disputes. Moreover, the online format dramatically reduces costs and timeframes, aligning with the UDRP's goal of providing an efficient, accessible, and economical alternative to court proceedings.

The online nature of UDRP proceedings, further replicated by SACI-Adm, also promotes procedural fairness and neutrality. In addition, the global accessibility of online proceedings ensures that both large corporations and individual domain name registrants—regardless of their geographical location—have the opportunity to defend or assert their rights effectively. The digital administration of disputes further supports transparency, as decisions are published online and contribute to the growing body of publicly available jurisprudence. Thus, the fully online structure of domain name dispute resolution is not merely a practical choice but a necessary adaptation to the decentralized, borderless, and instantaneous environment of the Internet.

Built in enforcement

Lastly, the success of the UDRP also relies on the built-in enforcement mechanism, which ensures that panel decisions are automatically implemented without requiring separate legal action.

Once a UDRP panel renders a decision ordering the transfer or cancellation of a domain name, the decision is binding on the domain name registrar, provided that no judicial proceedings are initiated by the losing party within ten business days. This automatic enforcement is critical because it allows for quick and effective resolution of domain name disputes, avoiding the need for successful complainants to seek court orders to compel compliance—a process that would otherwise undermine the efficiency and accessibility of the system.

By embedding enforcement within the contractual relationships between domain name registrars, registrants, and ICANN, the UDRP sidesteps many of the jurisdictional and practical difficulties that arise in international litigation. It ensures that administrative remedies have real-world effect without reliance on national court systems, which can vary significantly in speed, cost, and approach to Internet-related disputes. Furthermore, the threat of automatic transfer or cancellation encourages parties to take the UDRP process seriously, promoting compliance and discouraging frivolous defenses or deliberate bad-faith behavior. In this way, the UDRP's built-in enforcement is not merely a procedural convenience but a structural necessity for achieving its goals of efficient, fair, and globally applicable domain name dispute resolution.

Body of Case Law

Lastly, the framework established by the UDRP allowed the development of a robust body of case law, summarized by the WIPO Jurisprudential Overview [24], currently on its third edition. The great adherence of domain name dispute resolution mechanisms such as the UDRP created consensus views on a range of substantive and procedural issues, which assists the parties and panelists with predictability, offering clarity and consistency in decision-making. This body of case law also helps to discourage abusive claims.

Moreover, the development of a body of case law helps to refine legal standards and to clarify ambiguities, contributing to normative development and addressing issues such as free speech, criticism,

24 WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Jurisprudential Overview 3.0")

generic domain names, and better precise the concepts of "legitimate interests" and "bad faith". This fosters more predictable outcomes, streamlines dispute resolution, and ultimately, it supports the integrity and stability of the Domain Name System by promoting fair and efficient handling of domain name disputes, particularly in cases of cybersquatting.

Cited below are some leading cases decided on the early days of the UDRP which helped shape the jurisprudence applied not only to UDRP cases but also have been accepted by some ccTLDs:

Landmark cases:

Telstra Corporation Limited v. Nuclear Marshmallows, WIPO Case No. D2000-0003, <telstra.org>

- One of the earliest and most significant decisions under the UDRP, which developed the doctrine of passive holding.
- Trademark claimed: TELSTRA
- Domain name use: inactive

Australian telecommunications company Telstra filed a complaint against the respondent, Nuclear Marshmallows, for registering the domain name telstra.org. Telstra argued that the domain was confusingly similar to its registered trademark TELSTRA that the respondent had no legitimate rights or interests in the domain name, and that it was registered and used in bad faith.

Notably, the respondent had not developed a website or used the domain for any legitimate business purpose. The panel ruled in favor of Telstra, concluding that even passive holding of a domain name—where the registrant does not actively use the domain—can constitute bad faith under certain circumstances. The panel emphasized that Telstra's trademark was well known, and the respondent's failure to respond or provide a legitimate explanation supported an inference of bad faith. This case set an important precedent in UDRP jurisprudence by affirming that the absence of active use of a domain name does not preclude a finding of bad faith registration and use, especially when other factors point to an abusive registration.

Landmark cases:

Madonna Ciccone, p/k/a Madonna v. Dan Parisi, WIPO Case No. D2000-0847, <madonna.com>

- Established that a Respondent's trademark registration corresponding to a domain name does not automatically generate rights or legitimate interests in the domain name
- Trademark claimed: MADONNA
- Domain name use: initial use for a website with adult content

Parisi, a New York-based web developer who had registered the domain name madonna.com. Parisi had purchased the domain in 1998 for USD 20,000 and initially used it to host an adult entertainment website featuring sexually explicit content. He also registered the name "Madonna" as a trademark in Tunisia. In response to Madonna's objections, Parisi removed the explicit material and replaced it with a disclaimer stating that the site was not affiliated with Madonna, the Catholic Church, or other entities named "Madonna."

Despite these changes, Madonna argued that Parisi's use of the domain was in bad faith and sought its transfer. The panel ruled in favor of Madonna, concluding that the domain name was identical to her well-known trademark and that Parisi lacked rights or legitimate interests in the domain. The panel found that Parisi's registration of "Madonna" as a trademark in Tunisia was a strategic move to circumvent UDRP rules and did not constitute a bona fide use. Additionally, the panel determined that Parisi's intent was to capitalize on Madonna's fame for commercial gain, which constituted bad faith registration and use. As a result, the panel ordered the transfer of the domain name.

Landmark cases:

Oki Data Americas, Inc. v. ASD, Inc., WIPO Case No. D2001-0903, <okidataparts.com>

- Decision that established the concept that authorized resellers could be considered as having rights or legitimate interests in a domain name
- Trademark claimed: OKIDATA
- Domain name use: website offering repair services

Oki Data Americas, Inc. alleged that ASD, Inc. registered the domain name in bad faith, arguing that it was confusingly similar to its registered OKIDATA trademark. Oki Data Americas, Inc. contended that the ASD lacked a legitimate interest in the domain name and had no authorization to use the trademark in this manner.

The panel ruled in favor of the ASD, establishing a precedent that authorized resellers can have a legitimate interest in using a trademarked term in a domain name if the following conditions: (1) the Respondent must actually offer the goods or services at issue; (2) the site must sell only the trademarked goods; (3) the site must accurately disclose the Respondent's relationship with the trademark owner; and (4) the Respondent must not attempt to corner the market in all domain names related to the trademark.

The panel emphasized that the UDRP was designed to prevent cybersquatting and should not be used to litigate all disputes involving domain names. Trademark owners wishing to prevent the use of their marks by authorized sales and repair agents in domain names should negotiate such protections through appropriate contractual language or seek recovery in traditional trademark infringement or dilution litigations.

Conclusion

In light of the above, it is noted that the UDRP has not only become a cornerstone of global Internet governance but has also served as a vital blueprint for national adaptations, including country code top-level domain (ccTLD) policies such as Brazil's SACI-Adm. The UDRP's core elements—procedural efficiency, substantive clarity, low cost, and built-in enforcement—offered a framework that could be localized without sacrificing international legitimacy. Regional mechanisms like SACI-Adm also benefit from the UDRP's maturing jurisprudence. Ultimately, the UDRP's influence on ccTLD dispute frameworks underscores its normative power, not merely as a legal instrument, but as a model for adaptable, inclusive, and forward-looking digital governance. The SACI-Adm domain's dispute resolution mechanism reflects this influence while adapting to the Brazilian legal context, particularly in its integration of consumer rights principles and responsiveness to local stakeholders.

Looking towards the future, although artificial intelligence (AI), presents complex new challenges that will test the interpretative flexibility of domain name dispute resolution policies, creating new disruption to cyberspace, these new technologies also hold significant promise as a tool to enhance the efficiency and responsiveness of mechanisms that combat abusive domain name registrations. AI-driven technologies can support both proactive monitoring and reactive enforcement. For instance, tools inspired by services like DMCA Auto, which automate the detection and takedown of copyright-infringing content, could be adapted to identify suspicious domain registrations that are confusingly similar to trademarks, display patterns of impersonation, or are associated with known cybersquatting behaviors, offering an early-warning system to rights holders and registry operators. Such advancements would not only increase the accessibility of remedies for smaller rights holders but also help preserve the integrity of the domain name system by reducing reliance on manual enforcement. In any case, addressing these challenges effectively will require ongoing multi-stakeholder collaboration, ensuring that future revisions to domain name dispute policies reflect a balance of interests among trademark owners, registrants, technical experts, regulators, and civil society.

The Future of the Internet: A Tale of two worlds (controlled vs. open)

Konstantinos Komaitis

The first time I visited China was in 2006. I was invited to speak about how the Internet was managed and how decisions affecting its future were made. At the time, the World Summit on Information Society (WSIS) [25], the United Nations-led process that established the nexus between the Internet and the UN's development agenda had just concluded and it provided a blueprint for how the Internet were to be governed. Similarly, the multistakeholder model was recognized as the official arrangement for the management of the Internet's critical resources and collaboration was placed at the heart of ensuring that this new technology could only evolve in a way that was human-centric. It was a time when the Internet was celebrated for its openness, freedom and ability to advance human rights.

Not in China though.

In 2006, the Internet in China may have been rapidly expanding, both in terms of users and infrastructure, but it was also heavily regulated and censored by the Chinese government. The user base was growing fast, with millions of Chinese citizens going online each year, largely driven by urbanization and government investment in infrastructure. Many users accessed the Internet from Internet cafés, especially in rural and less wealthy urban areas. Home broadband was growing fast and DSL and cable broadband were becoming more common in major cities. Mobile was still in its early stages with the government heavily investing in telecommunications infrastructure as part of its modernization efforts[26]. The Great Firewall, China's main censorship machine, was already operational and was becoming more sophisticated, blocking and filtering access to foreign sites, including the BBC, Google and Wikipedia, while ISPs (and Internet cafés) were required to monitor user activity. [27] Topics

25 https://www.itu.int/net/wsis/

26 The Internet Timeline of China 2004-2006, https://www.cnnic.com.cn/IDR/hlwfzdsj/201209/t20120904_36017.htm

27 Inside the Great Firewall of China, https://money.cnn.com/magazines/fortune/fortune_archive/2006/03/20/8371819/index.htm

like Tiananmen Square, Falun Gong, Tibetan independence, and criticism of the Communist Party were strictly censored. Forums and bulletin boards, like Tianya and Mop, were popular spaces for public discussion and entertainment. Online gaming was booming, with MMORPGs like "World of Warcraft" and domestic titles gaining massive followings. E-commerce was still at an early-stage, but Alibaba and Taobao were growing fast. [28]

The second time I visited China was in 2013. By then, China's Internet way of networking was already one of the largest and most active digital ecosystems in the world, but it was heavily shaped by government policies, domestic innovation, and censorship mechanisms. The number of users had grown exponentially to around 600 million, making it the largest online population in the world. [29] Mobile Internet usage was booming, with a significant share of users accessing the web via smartphones, thanks to the rise of cheaper devices and 3G networks. In the meantime, the Great Firewall was in full effect, blocking access to many foreign websites including the New York Times, Google services, Twitter and, Facebook. The government monitored social media and websites for sensitive political content [30] and, because of this, Chinese alternatives were flourishing. This was the time, when Baidu started to dominate the search engine market, Tencent's QQ messaging was rapidly growing, while, WeChat a multi-purpose messaging, social media, and mobile payment app developed by Tencent had already amassed over 300 million users. Alibaba was establishing itself as the leader in e-commerce and Sina Weibo had become the most influential microblogging platform, similar to Twitter. By 2013, China's Internet was a paradox [31]: innovative and massive, yet tightly controlled. It had developed a parallel ecosystem to the global web, powered by domestic companies and shaped by government policy.

In 2013, however, China's Internet was the exemption. Outside of China, most of the users with Internet access, were able to experience a mostly open and global Internet and access to information and infrastructure

28 China surpasses the US in Internet Use, https://www.forbes.com/2006/03/31/china-Internet-usage-cx_nwp_0403china.html

29 China has more Internet users than any other country, https://www.pewresearch.org/short-reads/2013/12/02/china-has-more-Internet-users-than-any-other-country/

30 In China, the "Great Firewall" is changing a generation, https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation

31 David Talbot, China's Internet Paradox, MIT Review, 2010, https://www.technologyreview.com/2010/04/14/91784/chinas-Internet-paradox/

was generally uninhibited. However, growing concerns about surveillance, censorship, and control were starting to shape the digital landscape. Starting with the Edward Snowden's revelations [32] in June of that year, a series of threats were emerging marking a turning point for how the Internet would be perceived. Snowden's leaks exposed the NSA's global surveillance programs, including PRISM, which collected data from major tech companies, leading to an international debate about privacy, data sovereignty, and government overreach. At the same time, the consolidation of power among a few major tech companies, mainly Google, Facebook, Amazon and Apple, raised early alarm bells about gatekeeping, user tracking, and data monetization. Surveillance capitalism[33] was in full swing.

These events generated the perfect storm for a more intense interest and a deeper government intervention in the management of the Internet. Governments began to explore ways to exercise more control at different levels of the Internet stack: countries like China and Russia focused all the way down to the infrastructure, while others, like the European Union block, concentrated their attention to identifying how best to control the content that was circulating in the Internet. Control became the new buzzword and the Internet's new reality.

The thing about the Internet though is that it is specifically designed to avoid control. From a technical design perspective, every time there is an obstacle to the way packets of data get to move across networks, these packets will route around that obstacle taking different paths until they reach their destination. That's how the Internet is designed to behave. Unlike the telephone system where an obstacle, like a severed wire, would immediately disrupt communication, the Internet is characterized by redundancy and error correction mechanisms. While a temporary outage or network congestion can cause delays or failures, communication is less likely to be completely blocked like in a traditional analog system. In this sense, the Internet is not a monolith, but an ecosystem characterized by its complexity and resilience. It is an indefinite space where engineers, public policy experts, business professionals, researchers and advocates work together to form internetworking. In the Internet, every factor depends on every other factor, either directly or indirectly and a rule that affects the way protocols are created and deployed will often affect how networks interoperate and deliver data across borders. Businesses and users that

32 Edward Snowden: Leaks that exposed US spy programme, https://www.bbc.com/news/world-us-canada-23123964

33 Shoshana Zuboff: "Surveillance capitalism is an assault on human autonomy", https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

depend on such data will have to adapt to the changes, find another way to get that data or perish.

Over the years, the attacks against the open and free Internet have been multiple. Such attacks, which continue until today, target its architecture, its ability to grow and the ability of users to participate. Some of them are intentional while some are unintentional but, in the end, it really does not matter. The Internet – the way we are used to talk about it as one public, open space that provides global connectivity through interoperable building blocks – is eclipsing. In its place, different Internet models emerge driven by major geopolitical shifts.

Why is the one Internet important though?

The Internet is the most human technology to date. At its most technical level, the Internet, famously described as a network of networks, is a decentralized technology based on open standards. This design ensures a certain degree of resilience because it intentionally prohibits a central point of control over the way networks get to interact. [34] Just like us humans, very large networks, called Autonomous Systems (ASs), co-exist but, fundamentally, each is independent; open standards allow interoperation between the networks and this, in turn, ensures Internet growth. As long as a network agrees to use the open protocols and standards, there is no limit to the number of networks that can join the Internet. The more networks, the more diversity; and, the more diversity, the bigger the resilience. There is something profoundly human with the ability of ASs to create their own rules and processes, while, at the same time, being able to collaborate with one another. And, because they all want the same thing, they work towards that goal both collectively and independently. If Aristotle lived today, he would declare that "the Internet is, by nature, a social animal".

The initial vision of the Internet was a good one; but, today, it is getting dangerously lost. As governments became more invested in in its future, they have started gradually chipping away the its architecture, seeking to bespoke much of its design in a way that reflects their cultural, social and economic beliefs. SplInternet, [35] or the idea of having small Internet islands,

34 The Internet Way of Networking: Defining the critical properties of the Internet, https://www.Internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf

35 What is a SplInternet and why you should be paying attention, https://www.Internetsociety.org/blog/2022/03/what-is-the-splInternet-and-why-you-should-be-paying-attention/

is already a reality with Europe, the United States and China, all competing for how the Internet of the future should look like. These visions are driven predominantly by policies and regulations that are often conflicting, contradictory and are premised on notions of "digital sovereignty". [36]

Digital sovereignty refers to the ability of a country to control its own digital infrastructure, data, and policies, often to protect national interests, security, or cultural values. This includes regulating data flows, developing domestic technologies, and setting legal standards for how digital services operate within their borders. Countries asserting digital sovereignty may build isolated or heavily regulated Internet spaces resulting in Internet fragmentation, thus limiting cross-border communication and collaboration. This creates barriers to innovation and trade, in the sense that sovereignty-driven rules can require localization of data or infrastructure. In this context, small or foreign companies may find it hard to enter these markets, stifling competition and innovation. Moreover, under the guise of sovereignty, some governments implement surveillance and censorship policies, which restrict freedom of expression and access to information, key components of an open Internet resulting in national interests trumping collaborative decision-making, eroding global norms. Digital sovereignty is about control — often for legitimate goals like privacy and security — but when pushed too far, it can fragment the Internet, limit freedoms and undermine the global benefits of open digital ecosystems.

This kind of thinking is not novel. In *Seeing Like a State* [37], James C. Scott critiques "scientific forestry" as a key example of how modern states attempt to impose legibility and control over complex, organic systems. Using the example of scientific forestry, which emerged in 18th- and 19th-century Prussia and Saxony, and it involved reducing natural forests into rationalized, simplified, and standardized forms that could be easily measured, monitored, and exploited, primarily for economic gain, Scott seeks to demonstrate the detrimental effects oversimplification can have on complex systems.

Scott's analysis about the key aspects of scientific forestry could have been written for the Internet. Just like the Internet, natural forests are ecologically diverse and complex. Scientific forestry simplified this complexity by focusing only on the most economically valuable species (like oak or pine), arranged in neat rows and standardized units. All other

36 The Complexity of Europe's digital sovereignty agenda explained, https://dfrlab.org/2023/05/22/the-complexity-of-europes-digital-sovereignty-agenda-explained/

37 Seeing it like a state, https://yalebooks.yale.edu/book/9780300078152/seeing-like-a-state/

species, organisms, and ecological relationships were considered irrelevant or even obstacles. This simplification made forests "legible" to bureaucrats, allowing the state to calculate timber yields, plan harvests, and tax or manage forest resources more efficiently. But this came at the cost of ignoring local knowledge and ecological balance. While efficient in the short term, these rationalized forests often failed over time. Monocultures proved ecologically fragile, leading to disease, soil depletion, and reduced biodiversity. Scott calls this the "production of thin simplifications"—systems that seem efficient on paper but collapse in practice. Scientific forestry exemplifies how states simplify and standardize complex systems to make them more governable. However, in doing so, they often undermine the very systems they seek to manage. It's a cautionary tale about the dangers of high-modernist planning when it is detached from on-the-ground realities.

Similar attempts are now evident in the Internet. There is a race regarding which, and whose, values will prevail in the Internet ecosystem and how they will be applied. These competing values are idiosyncratic because they seek to transform the Internet into a monolith that fits neatly in separate jurisdictions; they attack its foundation for global, interoperable connectivity; and, they end up erecting borders and create chokepoints to the way networks can interoperate. In its effort to reach a level of legibility, the state neglects the Internet's own values and violates the normative rules that are necessary for the its health. Instead of celebrating its complexity, governments are seeing it as a problem. To this end and, despite its advancement, today's Internet feels less open, less global and less free compared to its early days.

There are two major frontrunners to this race. On the one hand, you have democratic nations that want to see the Internet continue to be open, global and interoperable; on the other hand, there are the authoritarian states that seek to impose an Internet model that is based on control and central authority. Each side views the Internet as a tool for achieving its own political, economic and social goals and, over the years, different policies and technologies have been deployed to reach that goal. To varying degrees, for both sides, the governance of the Internet is seen as a process of exercising political, economic and administrative authority in its development, diffusion and operation in society. Through a multitude of institutional and normative mechanisms, there is an attempt to steer Internet development within certain boundaries that reflect their values.

The current geopolitical environment does not help. Geopolitical dynamics are shifting the Internet from a global commons to a strategic asset subject to control, restriction, and fragmentation. While these shifts may serve national security and political aims, they run counter to the foundational principles of an open, interoperable Internet — ultimately

threatening innovation, economic efficiency, and global connectivity. As countries are prioritizing domestic tech industries and trying to reduce reliance on foreign technology, especially in areas like semiconductors, 5G, AI, and cloud infrastructure, divergent tech ecosystems are emerging, and the global flow of technology is becoming more restricted. At the same time, given the current international tensions, cyberattacks are increasingly being used as instruments of statecraft, eroding trust in digital infrastructure and making users more vulnerable to state-level surveillance and aggression. All this put a strain on the traditional multistakeholder model of Internet governance, thus making a tilt toward more authoritarian or state-controlled models possible.

Given the way things are evolving, we need to start building a new Internet coalition of leaders and, in this context, Brazil has strong reasons to position itself as a global leader for an open, global, interoperable, and secure Internet. As Latin America's largest economy, Brazil can champion Internet openness and digital inclusion across the region and is uniquely positioned to mediate between developed economies and emerging ones. Additionally, Brazil is uniquely positioned to represent the digital needs of developing nations while actively engaging with Western tech standards and governance. Advocating for an open Internet, not only aligns with Brazil's broader goals of reducing inequality and empowering marginalized communities but it is also part of Brazil's track record when it comes to advancing Internet freedom.

In 2014, Brazil became one of the first countries in the world to pass Marco Civil[38], a comprehensive digital rights law guaranteeing net neutrality, privacy, and freedom of expression. This was revolutionary and ,it continues to be, considering that, since then, no country in the world has managed to celebrate the Internet in such a way through a legislative action. Moreover, Brazil has been the host of major international initiatives and fora, like Net Mundial[39], that have supported multistakeholder governance models over authoritarian or purely market-driven ones. It is because of these things, amongst others, that Brazil has a vibrant digital economy [40], a thriving startup culture, and growing investments in AI and connectivity, making it a credible leader. Brazil is well-aware that an open, global and interoperable Internet boosts trade, innovation

38 https://www.cgi.br/pagina/marco-civil-law-of-the-Internet-in-brazil/180

39 https://netmundial.br

40 Brazilian Digital Transformation Strategy, https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/digitalstrategy.pdf

and competitiveness – all of which are vital for Brazil's growing economy and its integration into global markets. In this sense, leadership in digital governance can increase Brazil's soft power and attract more investment in its tech and data structure.

Ultimately, however, Brazil can be a major influence, especially considering its membership to the increasingly powerful BRICS block. It can be a democratic voice promoting an open Internet in contrast to models that favor surveillance, censorship, and control, like China's. It has the credibility, capacity, and geopolitical interest to lead on open Internet issues—and, doing so, would enhance its regional influence, support democratic norms, and unlock economic value for its people.

Choosing an open Internet is the right decision. An open Internet allows people to express ideas, share knowledge, and access information without censorship or unjust restrictions. This is a cornerstone of democratic societies and essential for informed public discourse. Threats like digital censorship, Internet shutdowns, surveillance, and the fragmentation of the Internet are increasing, and to this end, choosing an open Internet is a proactive stance to defend the digital public space we all rely on. In essence, an open Internet isn't just a technical or policy issue—it's a reflection of the kind of society we want to live in: one that values openness, fairness, and freedom.

Fighting for Words

Kathryn Kleiman

Introduction

The Internet I joined in college was a glorious space of educational speech, research and personal communications. It then became a place of great experimentation and innovation by young people with a great love of this Electronic Frontier and what it might become.

Belated, in the mid-1990s, big brands moved onto the Internet, some with intellectual property attorneys who seemed determined to drive everything off the Internet with which they did not agree. One area we fought over was domain names.

Domain names are the great street signs of the Internet. Like our street signs at home, they are an important way we can locate our local stores and restaurants, our schools, libraries and community centers, and they help us communicate our own personal ideas online.

Unfortunately, some large trademark owners did not come online until many short domain names were registered, and felt they could not get the "Internet street signs" that they wanted. They sought policies that would have taken domain names away from many other legitimate users – thus reducing communication of those without trademarks to a secondary status in the Domain Name System.

This is the story of how a few small groups in 1990s jumped in to defend the rights of registrants (those existing and not yet born). It is a story I have never told.

I. A Free, Open and Noncommercial Internet for colleges and universities

In the 1980s when I attended college, I received my first Internet account. I was a computer science student, and we got an email account to communicate with our professors and teaching assistants. Initially, we sent email to them, and then to each other. We realized that unlike the university hierarchies that limited our access to professors and administrators through strict hours and registration protocols, the Internet allowed us to reach them instantly. We could ask questions as they arose!

Eventually we realized that with email we could reach groups of students and even the entire campus. That was empowering because our ideas did not have to go through the editors of our newspaper or the managers of our campus radio station. Instead, we could send our notices directly to the entire student body – and we starting sharing events (now getting many more attendees) and our concerns for university policy changes (now getting much more attention).

Then we learned that the email accounts connected students and faculty around the world. Many of my friends also studied computer science and engineering and used their email accounts, and soon, we sent emails around the country and around the world – bypassing the expensive long distance telephone service of the day.

The Internet was magical and golden, a space for education and research, as well as personal and political speech. There was only one type of speech barred by the rules of the National Science Foundation, which ran the Internet at that time – commercial speech was not allowed.

A. Being Offline After College was Hard

Being offline after college was hard, for in those days, when you left the university, you lost your email account. But it was time to go to work, and I picked the most exciting place I could find – a Wall Street investment bank in New York City named Morgan Stanley.

I started my career in the Information Services Managing Training Program of Morgan Stanley – a long title for a program that recruited Ivy League graduates to help create the programs and systems that supported the millions of trades made every day by Morgan Stanley's traders and trading programs. What I learned is that we would run the data center and data communications of this great investment bank – and send information around the world.

But we had no Internet to use because commercial traffic was still banned from the Internet. What I also learned is that like the early days of computer programming when companies thought programming languages should be proprietary and not shared, some companies felt the same way in the late 1980s about their network protocols. While every university shared the same protocols, companies and countries did not.

This created a problem when we sent data around the world – for our networks in New York City run by IBM networks used IBM's protocol for data packets (SNA) and our European and Asian offices used the International Telecommunication Union's protocol for data packets (X.25) and gateways painstakingly translated the two forms and it worked most of the time.

But nothing works all the time, and neither did not local telephone loops in NYC, London and Tokyo, or the satellite uplinks and downlinks between the continents, and therein lay my job – receiving the calls from offices around the world at all times of day and night when the traffic slowed or stopped and figuring out if the break was mechanical, physical, logical or electrical and getting it fixed.

I remember wondering: Wouldn't it be simpler if we could all use the same network?

II. Internet Dot-com Innovators Began Creating a New Electronic World

Clearly there would be legal questions about the new world being created with all of this international telecommunications and data heading in all directions, and I decided to attend law school.

At Boston University School of Law, I studied the usual courses (torts, property, civil procedure) then dived into the courses that most interested me: administrative procedure for regulatory agencies, communications law, intellectual property law, international law and the US First Amendment (our laws of free speech). After working 14 hours a day on Wall Street, law school was fun and the three years went by quickly.

When I graduated, I joined the telecommunications law firm of Fletcher, Heald & Hildreth, located in Rosslyn, Virginia, just over the Key Bridge from Washington DC. We had glorious views of the Potomac River and the Iwo Jima Memorial (WWII) and were a dedicated group of attorneys helping telephone, satellite, microwave companies and radio and television broadcasters across the group get and keep their licenses with the US Federal Communications Commission. I was back working on networks, this time from a legal perspective, which I found fascinating.

A. The Dot-com Generation were Internet Pioneers

In the US, pursuant to a law passed by Congress in 1934, the Federal Communications Commission the public radio spectrum "in the public interest, convenience and necessity."[41] That was the work of my law firm and I enjoyed it.

41 U.S. Communications Act of 1934, 47 U.S.C. United States Code, Title 47 - TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS, CHAPTER 5 - WIRE OR RADIO COMMUNICATION

One special project helped our client, computer networking company 3Com, save the 2.4 GHz spectrum from auction for exclusive use by one company. Instead, we succeeded in preserving this spectrum for shared use, including for newly-invented wireless connections between computers and printers. This brilliant idea became the basis of Wi-Fi and Bluetooth, and we still use this frequency today.

My firm encouraged us to find clients, and I did. My friends included many computer scientists and engineers, and they, like me, were fascinated by the Internet they discovered in college. By now, in 1993 and 1994, NSF's restrictions against commercial speech online were slipping, and a few commercial connections were allowed online. A few Internet service providers provided commercial email accounts and services to entrepreneurs working on Internet matters, and the growing online service providers, including Prodigy, CompuServe and American Online (AOL) – behind their own extensive content and chat rooms quickly connected their email systems to the larger Internet.

We were back online, sending many emails, and watching our friends inventing new ways to use the Internet's resources!

One friend, Brad Templeton, a computer science graduate of the University of Waterloo in Canada, was well known for his joke list where he shared two excellent jokes once a week (noncommercial speech). He then decided to provide a service that his friends might need: if you gave him a keyword, like "telecommunications," he would search the newsfeeds and deliver articles directly about that topic directly to your email. It is a service we rely on every day now, but someone had to invent it and that was Brad through his new company Clarinet.

Brad needed good contracts with his news service providers, and on a holiday weekend when his main attorney was out of town, we worked together for two days to ensure that a contract renewal was finished and signed, so his service could continue. The new Internet businesses waited for no one.

Another client, a PhD mathematician, wrote mathematics puzzles and games for his daughter, and he thought other parents would be interested as well. There was a growing movement in the US to educate children at home, and he thought home schooling parents might want some challenging mathematical material for their children. On his Internet site, he gave away most of his educational games, but a few key puzzles he kept and sold for a small price (mostly to cover his Internet expenses).

My most dynamic new group of clients were the young Internet Service Providers – young professionals in search of higher speed telephone service to their suburban and rural homes. When the big

telephone companies would not provide them faster bandwidth (it was not cost-effective for residences in those days), they leased higher-speed lines themselves. Since I worked with T1 and T3 lines at Morgan Stanley, I spoke their language.

I also understood their concern that US federal regulations for telephone companies required "interconnectivity" (telephone companies leasing lines at reasonable rates), but the big telephone companies did not like or want the new ISPs and fought the rules directly and indirectly.

On behalf of the Internet Service Providers' Consortium (ISP/C), I joined multiple proceedings at the US FCC seeking to enforce their interconnection rights and lease many telephone lines for their Internet services.

These small ISPs began changing their rural and suburban areas. Because the T1 and T3 lines that they leased held too much capacity for one home, they shared and sold their excess capacity to local libraries and senior centers, community groups and their neighbors – regularly holding classes to teach seniors, children, teachers and neighbors how to use the Internet and handle the technical connections.

B. All People Need to Find Content on the Internet – and Drs. Paul Mockapetris and Jon Postel gave them a method

By now, in the mid-1990s, the Internet was beginning to grow. Senator Al Gore (later Vice President Al Gore with President Bill Clinton) wrote a bill to give NSF millions of dollars for Internet research and growth, in exchange for one major change. He wanted more commercial connections to the Internet.

Now the Dot-com community was growing quickly and because their work was still very new and innovative, the press dubbed this new era on the Internet "The Electronic Frontier."

1. The need for easily findable Internet addresses

The Internet now grew quickly and for people to easily find content, creators needed good, fixed online addresses. What we learned is that a decade earlier, two brilliant technologists, Drs. Paul Mockapetris and Jon Postel, solved an important problem. They knew that computers on the Internet sent and received data packets by using addresses with strings of unique numbers called Internet Protocol Addresses, or IP Addresses.

For example, an IP address looks like this: **13.107.246.40**, with the first set of numbers (on the left) being the "network ID" and the last three numerical fields being "the host ID." Every data packet sent to this IP address – currently assigned to American University – will arrive at the destination of my university to be reassembled into a full email or file and delivered to a student, faculty to staff member. All IP addresses must be unique across the Internet (then and today).

But people do not remember long strings of numbers well, and Dr. Mockapetris created an easier way for us to easily communicate with many IP Addresses without remembering them. He allowed the creator of Internet content to choose a unique set of letters and numbers, and then he created a routine to BIND them to an IP address.

Thus, when someone types my email address, Kleiman@AMERICAN.EDU, the browser routes to a table, finds the IP address of AMERICAN.EDU, and sends the data packets 13.107.246.40, to be assembled in order and delivered to my inbox.

BIND worked quickly and invisibly to us, and gave us powerful underpinnings for the current Internet addressing system. Dr. Postel gave form and meaning to these new letters and numbers. Under contract for the National Science Foundation in 1985, he set up seven generic top level domains to loosely organize our speech online: .COM, .ORG, .NET, .GOV, .EDU, .MIL, and .INT. This is one of the great inventions of the 20th century.

For with Dr. Mockapetris' table and Dr. Postel's generic top level domains, each top level domain can have its own table, and each second level domain name maps to its own table and IP addresses. Ditto for levels three, four and more. Thus, WCL.AMERICAN.EDU, a third level domain of AMERICAN.EDU maps to the IP address of American University Washington College of Law and allows my students to reach their law school information and class website.

It is very well organized, orderly, and well-designed to allow us to send messages – via data packets – quickly to their destinations across the Internet.

2. All of my Dot-Com Clients Needed a Way for People to Find Them on the Internet – they All needed Domain Names

Thus, Dr. Postel created the street signs of the Internet: Domain Names. Initially, the stories say, he gave out domain names himself

and tracked the names and their IP addresses on a pad he kept in his pocket. Obviously, that was not a recipe for growth, and by the early 1990s, NSF paid a small company named Network Solutions, Inc., in Northern Virginia, for each registration.

The top level domain that really counted in those early days (late 1980s, early 1990s) were .GOV for US government agencies savvy enough to be online and .EDU for the many colleges and universities now coming online. The military used .MIL for its own purposes – and we could not access its networks or work.

But .COM, .NET and .ORG (.COM for commercial, .NET for technical, and .ORG for noncommercial, loosely as there were no formal screening mechanisms) were of great interest to my clients. For they all needed street signs on the Internet for customers and readers to find their services and information, and sign up to receive more.

Network Solutions cleverly came up with a new idea for NSF: Rather than NSF paying for each domain name registered, Network Solutions could charge these entrepreneurs for each domain name registered in .COM, .ORG and .NET, and Network Solutions would pay NSF a part of the money received (plus register the .GOV and .EDU domain names for free).

It was a good deal, NSF agreed, and commercial domain name registration was born! My clients were happy to pay $50 a year/2 year minimum because domain names, for them, were a novelty and a necessity. They were the first street signs of the Electronic Frontier, and some of their domain names became famous:

- CLARI.NET – for Templeton's keyword new service
- PONY.COM – for the mathematician's mathematical puzzles website (his daughter loved puzzles)
- PETA.ORG – for Internet pioneer Michael Doughney's "People Eating Tasty Animals" parody of People for the Ethical Treatment of Animals (an anti-animal testing, anti-animal eating, anti-animal pet group that already had its own domain name, petaonline.org).

For the young Internet Service Providers that I and others represented, their domain names were the key, not only to their own business, but to the activities and businesses of others. For in those days, domain names were rare and a subscribers' email address "hung off" its ISP's domain names, e.g., KATHY@ISP.COM. Like many entrepreneurs, the ISPs

sought short, memorable domain names for their companies. For example:

- ROADRUNNER.COM (not my client) choosing Roadrunner as the very fast bird that runs in the desert of New Mexico where the company was founded, and

- BIGAPPLE.COM (my client) choosing "Big Apple" for its home in New York City (nicknamed the Big Apple) and its pride at being the first Internet Service Provider to serve its community there.

Gradually the world became more familiar with the internet and the new street signs of our electronic roads. More and more people were coming online and my clients with their commercial and noncommercial services were growing, teaching and helping change the Electronic Frontier into a richer, more diverse, broader community.

I was certain a new golden age of a new technology and telecommunications was on the horizon and in 1995, I convinced my firm to create an "Internet Law & Policy Group," one of the first legal groups of its kind in the world.

III. The Most Misunderstood Magazine Article of a Generation and the Empire Strikes Back

An unusual group did not join the hubbub of online activity. Big business did not realize that the Internet was worth paying attention to, and in the early to mid-1990s, few major companies existed online.

Registration of domain names, now by a small company named Networks Solutions.

Meanwhile, in the mid-1990s, Network Solutions served as both registrar and registry– selling domain names to the public and managing the database that mapped its domain names to the IP addresses of email and file servers. They continued the policies that Dr. Postel set out for domain name registration and NSF maintained: First-come, first-served for domain name registration. While .EDU and .GOV were limited in their registrations, .COM, .NET, and .ORG now were open!

All was going swimmingly, Internet innovation and experimentation was growing, and everyone seemed happy with this new Electronic Frontier. Groups formed to help us map out the rights and responsibilities of people online, including the Electronic Frontier Foundation (EFF). I was happy with my work in old and new communications technologies.

Then on October 1, 1994, Joshua Quittner published an article in Wired Magazine, the then-cool new magazine about new technologies, culture and policy read by entrepreneurs and policymakers. It is the most misunderstood article of the last thirty years.

For Quittner had noticed what the rest of us knew: Large companies were not paying much attention to the growing Internet, and he thought that was a mistake. How could a multinational company, rapidly opening restaurants around the world, not pay attention to a communications technology that was rapidly bringing people online around the world?

In the characteristic extreme manner of this young magazine, Quittner set about not only to write about a problem, but to illustrate it. He got the attention of a billion dollar company in an impossible-to-ignore manner: He registered the domain name MCDONALDS.COM.

He then wrote a story teasing the billion dollar hamburger company about being slow to see the incredible international opportunity of the Internet. He opened the article with the sentences:

> "I'm waiting for a call back from McDonald's, the hamburger people. They're trying to find me someone - anyone - within corporate headquarters who knows what the Internet is and can tell me why there are no Golden Arches on the information highway."[42]

Unfortunately, Wired poked the sleeping giant a little hard by titling the article "Billions Registered" as an exaggerated reference to domain names registered (even today, we do not have a billion domain names). The title was clearly a reference to McDonald's slogan "Billons Served," which we all knew.

But Quittner's subtitle, for the trademark attorneys serving the largest companies in the world issued what seemed to be a threat: *"Right now, there are no rules to keep you from owning a bitchin' corporate name as your own Internet address."*

Suddenly, the largest companies in the world, and their very large law firms woke up, and like people jolted awake by a very loud noise, they were not happy and angry at the person who issued the alarm and everyone around him.

Suddenly, the cry of "cybersquatter" rent the air. For Quittner had not just written about a problem, but he had registered a domain name

42 Billions Registered, Wired Magazine
https://www.wired.com/1994/10/mcdonalds/

and thus become part of the problem, according to the newly-awakened attorneys. "Cybersquatter" became the word they threw at him and at everyone who came onto the Internet and registered domain names before their clients – especially domain names that looked or sounded a little like their clients' trademarks.

A. But trademarks can be names that many people use for many things.

The problem, though, is that domain names are not trademarks (they are mnemonic identifiers for IP addresses) and that trademark owners do not "own" words. They file to use a certain word, set of words, or logos in commerce in a particular category of goods and services. Thus, in the US, "Wendy's" is the name of famous and excellent hamburger and chili restaurant (the first one was in Columbus, Ohio, where I grew up and we were very proud of it).

But just because the Wendy's restaurant exists, that does not mean that I cannot name my daughter Wendy. Nor does it mean that a playwright cannot name their play "Wendy" if they decided to write about the girl who befriends Peter Pan in the famous British story. Even the globally-famous McDonald's brand cannot deprive the tens of thousands of people from Scotland and of Scottish descent from using their last names in the regular course of life, including registering for schools, become professionals using their last names, and opening up other businesses that are not hamburger restaurants, such as Jane McDonald Accounting or Jim McDonalds Catering.

B. Trademarks can be ordinary dictionary words or geographically descriptive words open for all to use in the normal course of conversations and writings.

I remember attending one conference in these days after the article when trademark attorneys, furious at having missing something for their clients, lashed out and declared that anything that used "their client's words" in domain names was illegal, and I pointed out again and again that that could not be true because their clients' words were also dictionary words and belonged to everyone: Delta Airlines started 100 years ago as a crop dusting company in the Tennessee Delta, a famous US river valley. Delta can use the word for airlines, but it cannot take it away from the Tennessee Delta region for geographic use.

C. There was a profusion of panels about cybersquatting where many seemed to vehemently agree, except me.

Panel after panel, conference after conference, speaker after speaker in those busy months and years told us (and lawmakers) that cyersquatters were terrible, the world was coming to an end, and words in domain names belonged to the largest, richest trademark owners (regardless of who registered them first, how long they had been using them or for what purpose they were registered).

I tried again and again to explain how my clients were the first in their fields to use these domain names for their speech – both commercial and noncommercial – and removing their domain names arbitrarily would be a huge miscarriage of justice and huge mistake for our economy. It would result in many small companies being taken down and much speech being lost. But the large companies and their trademark attorneys did not care. We were all "cybersquatters" as far as they were concerned.

D. Can the trademark of a company purposely be used in a domain name now owned by that trademark owner? The answer is yes.

I remember a Price Waterhouse domain name conference where I was mentally tired of the same arguments and physically tired because I was about five months pregnant. At the conference, speaker after speaker condemning domain name registrants and finally it was my turn to come to the podium. I shared my thoughts about domain names, entrepreneurs, first-come, first-served, and the need to bring onto the Internet the same principles that govern speech and trademark in the real world.

I opened for questions and immediately was asked:

"Didn't you agree that any domain name that contain a company's trademark should be taken down?"

I did not hesitate to say "no" and offered an example that occurred to me in that moment. In the evenings at home, I had been researching cribs for my future nursery and the safety of various brands. If despite all my research, I purchased a crib and its slats were not properly arranged to be safe, and if my future baby died because his head stuck in the slats, then the very next day I would register the domain name CRIBNAMEKILLS.COM to let every new parent know about the danger of this device and the need to protect their children from it.

Not only was this use of a trademark in a domain completely legal, it was fully protected by the US First Amendment that ensures rights to free speech and the right to share full and honest information – even if it is deeply critical of a good or service.

I was clearly very pregnant as I shared this response, and there was dead silence in the room.

E. Under trademark law, the duty of policing belongs to the trademark owner

In the real world, trademark law imposes the duty of policing on the trademark owner, not the rest of the world. I may name my children, non-profit organizations, companies and their goods and services as I see fit, and choose the best names for my goods and services. If a trademark owner finds my use to be "infringing," then they can bring a lawsuit in court and make their case.

But trademark lawyers know that big companies have lost infringement cases for many reasons, including that the defendant used the word in a very different way, directed its use to a different audience, was in a different country, or had a legitimate noncommercial use.

Plus, every large company deeply fears that their brand name could become "generic" and be declared such by the court. When brand becomes generic, even the most famous trademark is no longer protected because the word had become the name of a category of goods and services (and no longer serves as a source identifier to the company). Every student studying trademark law learns the famous brands that became generic words, including "thermos," "escalator" and "elevator."

But as the old folk song says, "Now the valley cried in anger, mount your houses, draw your swords," [43] and the trademark owners formed committee after committee and lobbied the US Congress for rules allowing them to revoke domain names at will, not just for coined and fanciful terms (very strong trademarks) like Xerox, Exxon and Häagen-Dazs), but ordinary words like American, United and Orange.

Frankly, I think the pushback came as much from embarrassment as anger. The big companies and their attorneys missed the growth of something new, and were late to the online party.

43 One Tin Soldier song, lyrics available in numerous places, including: https://genius.com/The-original-caste-one-tin-soldier-lyrics

F. Cybersquatter was misused against Quittner, then and today, but he and McDonalds trademark attorney got past the problem years later (perhaps we can too).

Cybersquatters because a slanderous name for registrants with domain names that a trademark owner or their attorney wanted. It was true then and, unfortunately, it continues to be true today as we heard the old insult hurdled on stage on April 23, 2025, at a meeting held by the World Intellectual property Organization. Once again, reporter Joshua Quittner, and others, were called cybersquatters; once again they were wrong.

For the term does not make sense against Quittner or many of the groups and individuals against which it is used. Quittner registered the domain name MCDONALDS.COM – for the legal purposes of criticism and commentary – to point out that a multinational hamburger company was missing a multinational opportunity. It was clearly free speech commentary.

Further, he did not want to keep the domain name and offered to transfer the domain name to McDonalds Corporation for two computers donated to his daughters' school. Years later, he and David Maher, then senior trademark for McDonalds met for lunch to discuss this explosive period of time. By then, Maher was a self-described "recovering trademark attorney." They laughed about old times, and mended bridges. I wish everyone in our community could mend bridges as professionally and positively.

IV. Threats, a New Domain Name Dispute Policy, and a New Organization seeking balance and fairness, the Domain Name Rights Coalition

By now, in 1996 and 1997, as the word "cybersquatter" was brandished by every trademark attorney who wanted a registered domain name, my clients became to receive "cease and desist" letters on even the most basic words in domain names.

A. Professional cease and desist letters and traditional trademark bullies.

I had worked with cease and desist letters on behalf of my telecommunications clients, and they were generally quite professional.

One radio station would notice that another radio station was using the same name or slogan and write to my client asking them to change their name or slogan.

I would do the research, find that the two radio stations were located thousands of miles from each other, had no overlapping signals, and thus there was no consumer confusion. I wrote back on behalf of my clients, pointing out these facts, and normally, the issue ended there.

Once I saw a trademark bully – the new NFL team named the "Panthers" came into Charlotte, North Carolina, and used cease and desist letters to try and drive out other "Panthers" in the area, including high school teams using their mascot name for many years.

The NFL then targeted my firm's longstanding client, a small radio broadcaster in the region for its his long-standing slogan, "Home of the Panthers." The cease and desist letter was strong and threatening, but our client was patient and smart. He asked us to do the research: Did he have to change his slogan, "Home of the Panthers," a slogan he had used for years and his customers knew well?

I did the research and the answer was a clear no. The radio station was the prior user of this mark in this area. Further, in the basement of US Patent & Trademark Office (USPOT), I found that NFL Team's application for this trademark had originally been rejected. The NFL Team ultimately received the trademark by persuading the USPTO that they were entering a "crowded field," and thus, would join and share this field with the many existing users of "panther" and "panthers" in the area – a commitment they did not honor.

With this research, my client went to court and a federal judge agreed with him – although the radio station was much smaller than the NFL, trademark law was still on his side and he could continue to use his slogan. *He won, but this was a very expensive way to protect his business. Requiring all Internet entrepreneurs and organizations to go to federal court to protect their domain names would be an impossibly expensive hurdle to place in front of individuals and small groups starting out in the Electronic Frontier.*

B. The cease and desist letters against domain names became intimidating and utterly unprofessional

The cease and desist letters sent to my Internet clients seeking their domain names were not as polite or well-reasoned as the radio broadcaster ones. These letters were threatening, mean, and intimidating. Most warned of ridiculous penalties, including jail and racketeering charges, for domain names that, in many cases, were dictionary words and common names. Some examples:

- Pony International, an athletic footwear and clothing company, wrote demanding my client's PONY.COM domain name used for his educational software website;

- People Eating Tasty Animals called for Michael Doughney to immediately take down PETA.ORG to takedown his parody – a wonderful website with links to national and state parks with hunting and fishing, humane societies helping homeless pets find new families, and testing involving animals; and

- BIGAPPLE.COM received a cease and desist letter from another company located in NYC, with very different goods and services, that just told it to go away and hand over the domain name.

It was not just us. In 1995 and 1996, registrants were getting demands for their domain names and then, like today, they knew it would be hard to keep their audiences and customers if they suddenly changed their addresses. For their domain names were shared on their business cards and brochures, advertisements and conference materials.

A consensus was growing that we needed a formal policy to help.

C. Network Solutions adopted the NSI Domain Name Dispute Policy and we created the Domain Name Rights Coalition.

Dot-com pioneers were not the only ones getting threats about domain names. The billion dollar company Lockheed Martin threatened Network Solutions – the registry/registrar - ordering it to remove any domain names for Skunk Works, an advanced technology division of Lockheed Martin (and similar terms), and to "pre-screen" and refuse to register future domain names with those words.

Network Solutions, of course, was not in a position to do so. First-come, first-served registration is the policy it was told to adopt, and especially after Lockheed Martin sued Network Solutions in federal court (Network Solutions won) and the National Science Foundation did not help or support them, Network Solutions knew it was on its own and had to do something. [44]

In mid-1995, Network Solutions quietly adopted a domain name dispute policy to allow it to revoke and transfer domain names. Although federal rules require government agencies to adopt rules through open and public processes, NSF created these rules behind closed doors, likely influenced by the groups they feared most, the largest trademark owners.

For the Network Solutions Domain Name Dispute Policy [45] continued NSF's policy of first-come, first-served registration, but allowed any trademark owner with a certified federal trademark from any country in the world, to challenge an existing domain name.

This was the procedure:

1. After the complaint was filed, and its documents checked, Network Solutions sent a letter to the registrant stating the complaint against the domain name, and giving them 30 days to produce their own federally-registered mark.

2. If they did produce a certified federal trademark (from any country in the world), then NSI would take no action.

3. If the registrant could not produce a federal trademark, then Network Solutions would transfer the domain name to the trademark owner.

This policy was unfair, imbalanced and inconsistent with trademark law. First, trademark law provides registrations for commercial purposes – we have never been required anywhere in the world to obtain trademarks for our noncommercial speech – personal, political, educational, research, hobbies and activities – because they are not eligible for trademarks under law (in many cases).

44 Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949 (C.D. Cal. 1997), affirmed, Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980 (9th Cir. 1999)

45 No link to the NSI Domain Name Dispute Policy of July 28, 1995, appear to exist. See e.g., ftp://rs.internic.net/policy/internic/internic-domain-1.txt.

Further, even for those who are eligible for trademarks and meet the high standard (which in the use includes interstate commerce), they could not obtain them. For at that moment in time, the US Patent & Trademark Office had a two-year backlog. They did not have enough staff to process pending trademark applications, and many of my Dot-com pioneers were stuck in the queue. But a "pending trademark application" was not a defense under Network Solutions' rules to a trademark owners' complaint.

Nor was the response that "this is my name" or "I'm using this domain name term in a completely different way than the trademark in the complaint" or I am using my domain name for noncommercial speech. Under Network Solutions Domain Name Dispute Policy, you either had a federal trademark or you did not; you either kept your domain name or you did not.

Carl Oppedahl, attorney for the Roadrunner Internet Service Provider, heroically filed in federal court to stop Network Solutions from transferring ROADRUNNER.COM to Warner Brothers. The Federal Court agreed with Oppedahl that Internet Service Providers using the fast bird and Warner Brother's famous cartoon character of the fast bird were very different and ordered NSI not to transfer the domain name under its rules.[46]

But my clients had no such resources to go to federal court (a process that takes tens of thousands of dollars or more), and having to go seemed a terribly high price for an entrepreneur, small business, small organization or individual to pay for the privilege of offering education, research, and other forms of information, services and products online.

It seemed a violation of public policy and the public interest to force new entrants to pay such absurdly high prices could kill our Dot-com community and threaten the future Internet environment and new organizations of many types.

D. In 1996, we founded the Domain Name Rights Coalition.

In 1996, we did the only thing we could think of, we founded an organization that we named the Domain Name Rights Coalition. Michael Doughney, co-founder of one of the first Internet Service Providers in the US named Digex, Michaela Barry, co-founder of InterCon Systems

46 Roadrunner Computer Systems, Inc. in Roadrunner Computer Systems, Inc. v. Network Solutions, Inc., 96-civ-413-A. (E.D. Va. filed Mar. 26, 1996).

Corporation, a pioneering software company creating online products for Macintosh computers, and I were founders. The goal of the group, DNRC as we called it, was to protect these Internet street signs and the full range of noncommercial and commercial speech that used them. Our logo was a street sign.

To my surprise, Network Solutions' General Counsel, Philip Sbarbaro, was not upset when I visited him to share the purpose of our group. Instead, he invited me to join him on panels to discuss domain name problems and to these discussions, I brought DNRC's call for fairness and balance. Together, we attended panels of Virginia State Bar and Virginia Bar Association, and more, and discussed concerns about registrants, trademark owners and domain name dispute policy.

Later, Sbarbaro wrote that during these years, he felt being caught in a "shootout" between Internet innovators and big businesses. I hardly think we had the fire power of the big law firms, but he drew on an old image of rivalry in the US in the late 19th century:

> "Picture yourself in a wide, fast-running cold water creek between two mountainsides, one populated by the Hatfields and the other by the McCoys. As you stand knee-deep in that freezing current, which seems to be rising rapidly, look up one side at the McCoys, rifles loaded, cocked and aimed. Directly across the creek stand the Hatfields, equally prepared. Some of those rifles, more than you can count, are aimed directly at you. Call yourself "the Registry." [The "real McCoys" are the trademark owners and the Hatfields represented those using domain names "unaccosted and without interruption for months or years, either in business or simply as a communications device…"]. [47]

E. Michaela Barry and I spoke with a variety of additional groups and forums, and Congress.

Separately, Barry and I went to other groups and meetings. I gave presentations at the DC Bar Association and the Federal Communications Bar Association. Barry went to Singapore to speak about domain name streets signs. She remembers being swung around by John Perry Barlow, lyricist for the American rock band, the Grateful

47 Unpublished paper available written by Philip Sbarbaro shared with author.

Dead. and co-founder of the digital rights group, the Electronic Frontier Foundation, who dramatically shouted: "I understand now. Domain Names are Speech."

Our message shared basic principles of language, free speech, and trademark law with all who would listen, and fundamental principles: Dictionary words belong to everyone and law protects our right to use our own names in most circumstances. Trademarks were never meant to displace language and domain names need to serve everyone.

Further, we asked as a matter of public policy, shouldn't our policies encourage new organizations, entrepreneurs and individuals to use the Internet for their speech and communication, and not threaten them with arbitrary revocation of the domain names that their families, friends, communities and customers used to find their content online?

In June 10, 1998, I testified before a Congressional committee about the damage we faced with current unbalanced and unfair policies:

> "Without the equities of traditional trademark law, we fear that small businesses, individual and entrepreneurs will continue to forced off the Internet along with the robust speech, ideas, and services that they offer." [48]

F. Innovative and unusual ways to respond to cease and desist letters

I continued to respond to numerous cease and desist letters, sometimes with humor, sometimes with counterthreats. To one unduly threatening letter, I proposed reading the letter on the Tonight Show, a popular national nighttime comedy show, as I expected the entire world to laugh (it was a common three-letter word that the letter was demanding with outrageous threats).

In response to another letter, sent to a young doctor, I worked with EFF to create a "Hall of Shame" and induct this very large company into it for unfair and unreasonable trademark practices.

In both cases, saner voices soon joined us from the large companies (and their marketing teams) and helped the trademark lawyers settle

48 Hearing on Electronic Commerce: The Future of the Domain Name System Before House Subcommittee on Telecommunications, Trade, and Consumer Protection, 102nd Cong. (June 10, 1992) (statement of Kathryn A. Kleiman, General Counsel, A-TCPIP/Domain Name Rights Coalition).

the matters in a reasonable fashion. But our goal seeking the revocation of Network Solutions' Domain Name Dispute Policy remained elusive. We needed to do more.

V. A New Organization to Oversee Internet Identifiers and two new Organizations to Seek Fair and Balanced Domain Name Policies for Registrants

In the midst of fights, NSF decided to exit oversight of the critical Internet identifiers. NSF left quickly and turned over its roles to the US Department of Commerce. On July 2, 1997, Commerce issued a request for comments on the "administration of Internet domain names" and indicated a new direction – possibly private management and oversight.

Domain Name Rights Coalition jumped in, filed comments, and called for protection of all registrants. Together with the telecommunications public interest group NetAction, we wrote:

> "DNRC and NetAction warn that if trademark law becomes overbroad on the Internet, making the only protected users of domain names large trademark owners, then the Internet will wither from a robust and diverse community into an abandoned cyberspace shopping mall." [49]

We called for express protection of speech and online domain name use of schools, libraries, individuals and small businesses in all future policies.

A. The Green Paper

On January 30, 1998, a part of the Department of Commerce called the National Telecommunications and Information Administration (NTIA) issued a new and more detailed Proposal to Improve the Technical Management of Internet Names and Addresses, nicknamed the Green Paper.

NTIA received more than 650 comments, including DNRC's 50 page comment.

49 Comments on the Registration and Administration of Internet Domain Names, US Department of Commerce, Comments of the Domain Name Rights Coalition and NetAction, August 18, 1997.

The Green Paper posited a new and private organization to manage and oversee the Internet's key identifiers (IP Addresses and domain names) and protocols associated with them, but we did not think the "principles" for these organizations were sufficient. In addition to:

Stability	Private bottom-up coordination
Competition	Representation

DNRC wanted to see clear and strong protections for free speech and civil liberties. We wanted to see a domain name-trademark policy created by a fair and neutral forum, one understanding the needs of big trademark owners, and future trademark owners, and noncommercial and commercial speakers online, including individuals. All would need their domain name street signs.

B. The White Paper and Its Final Rules Privatizing Internet Identifiers, including Domain Names

In the final version, NTIA's Statement of Policy on the Management of Internet Names and Addresses, nicknamed the White Paper, and published on June 05, 1998, NTIA, the US Department of Commerce and the Clinton Administration committee committed to a bold new direction for US policy:

We were assured:

> "Existing human rights and free speech protections will not be disturbed and, therefore, need not be specifically included in the core principles for DNS management." [50]

Then, with a sigh, we noted that the "U.S. Government will seek international support to call upon the World Intellectual Property Organization (WIPO) to initiate a balanced and transparent process, which includes the participation of trademark holders and members of the Internet community who are not trademark holders."

We wondered how fair and balanced it would be?

50 *Statement of Policy on the Management of Internet Names and Addresses.* Date of Publication, June 05, 1998, https://www.ntia.gov/federal-register-notice/statement-policy-management-internet-names-and-addresses

C. WIPO made policies for the largest companies in the world and Professor Michael Froomkin complained eloquently and comprehensively.

The World Intellectual Property Organization is not somewhere moist noncommercial organizations or small businesses spend their time or energy. It is a place where governments and large intellectual property owners meet to seek treaties and international cooperation for intellectual protection, including trademarks.

WIPO set up an Advisory Committee, but it was not very balanced. After an outcry, they added a young law professor who studied civil liberties, but not, by his own admission, trademark law. [51] The Advisory Committee, under the leaders of later Secretary General of WIPO, Francis Gurry, went out around the world to listen to presenters.

As you would expect, the WIPO Advisory Committee, in its meetings around the world heard mostly from attorneys for large companies and large law firms because that is who their communication reached. I remember attending the hearing in Washington DC and spending the better of the day, like the WIPO Advisory Committee, listening to speaker after speaking talking about cybersquatting, the world coming to an end, and the clear need for trademark owners to seize domain names as quickly as possible.

When my turn came to go to the microphone in the large auditorium, I got up and began to talk about free speech, fair use, noncommercial use, and the needs of entrepreneurs in the future, as with all entrepreneurs in the past, to name their goods and services and use the same dictionary words and names used by everyone. A domain name was not a trademark, and we needed very carefully balanced policies before we yanked them away, and took away someone's webpages, email addresses, and listservs – someone else's speech.

I looked like a corporate lawyer (in my best blue suit), but I didn't sound like one. Initially, there were polite smiles, but soon, they realized they were not hearing what they expected to hear and unintended looks of shock and surprise flashed across the Advisory Committee members' faces. I was not telling them what others told them; I did not feel very welcome in this forum.

51 Semi-Private International Rulemaking: Lessons Learned from the WIPO Domain Name Process, ver. 2.0, A. Michael Froomkin, https://osaka.law.miami.edu/froomkin/articles/tprc99.pdf

D. The WIPO Advisory Committee met privately, and its newest member was very upset.

The WIPO Advisory Committee met, it is clear from his writings, that Professor Michael Froomkin voiced deep concerns about the deep and long term harms of policies being proposed, and did not receive the attention to his concerns, or the changes he thought were needed.

In early 1999, Professor Froomkin did the unthinkable. He published his concerns about the WIPO proceeding and where it was going. He did so in a way that was elegant, academic, strong, clear, supported and utterly heroic. In his writing, A Critique of WIPO's RFC 3, he shared:

> "The World Intellectual Property Organization's plan to restructure the way Internet domain names in .com, .net, and .org are assigned and adjudicated is deeply flawed…
> WIPO was asked to make suggestions for better dispute resolution, and it claims to have produced a plan that creates no new rights for intellectual property owners. In fact, however, the plan would impose extensive Alternative Dispute Resolution on all domain name registrants accused of infringing of any type of intellectual property with their registration."

Froomkin then listed "The WIPO plan's flaws", including: [52]

- Bias. The plan is biased in favor of trademark holders;
- Enabling censorship. The WIPO plan fails to protect fundamental free-speech interests including parody, and criticism of corporations;
- Zero Privacy. The WIPO plan provides zero privacy protections for the name, address and phone number of individual registrants;
- Intimidation. The WIPO plan creates an expensive loser-pays arbitration process with uncertain rules that will intimidate persons who have registered into surrendering valid registrations;

52 Froomkin, A. Michael, A Critique of WIPO's RFC3 (1999). Available at SSRN: https://ssrn.com/abstract=2715738 or http://dx.doi.org/10.2139/ssrn.2715738

- Tilts the playing field. The WIPO plan would always allow challenges to domain names registrations [sic] to appeal to a court, but would often deny this privilege to the original registrant;

- Smorgasbord approach to law. Instead of directing arbitrators to apply applicable law, WIPO proposes using additional, different, rules it selected-rules that will often disadvantage registrants."

In 52 riveting pages, Froomkin laid out how much was being given away behind closed doors and what it would cost the rest of us. He shared ideas, changes, and revisions, but the most valuable part of this incredible paper was throwing open the doors to the closed room of the WIPO Advisory Committee and shining a light on just how much of our rights they meant to give away.

E. WIPO Forum in DC – Round 2

I can only imagine the retribution Froomkin faced in the back room, yet his actions helped vital information and helped move the WIPO committee off some of their more extreme positions. The world owes him an enormous thanks.

In the next public consultation in Washington, DC in early spring 1999, we were ready to speak in greater numbers: Michael Doughney, co-founder of the Domain Name Rights Coalition spoke about small businesses, parody, and noncommercial speech.

Eric Menge of the US Small Business Administration pointed out the problems he saw:

> "as of November 1998, 41% of all small and mid-size businesses in the USA have a website, and 22 percent of those businesses use the Internet to sell goods and services." He did not want to see them lose their domain names just because they did not yet have a registered trademark." [53]

But in the end, the WIPO Advisory Committee paid little attention to our concerns for fairness and balance and protecting

53 Footnotes 210 and 211, THE MANAGEMENT OF INTERNET NAMES AND ADDRESSES: INTELLECTUAL PROPERTY ISSUES, Final Report of the WIPO Internet Domain Name Process, April 30, 1999, http://wipo2.wipo.int

future generations of Internet users. The Committee adopted only some of Professor Froomkin's suggestions, very few. In the end, the policy WIPO delivered was still very one-sided: biased for large trademark owners.

VI. The New Organization of the Internet Corporation for Assigned Names and Numbers (ICANN) and two New Organizations to Protect Noncommercial Speech and Domain Names Online.

WIPO handed the policy to the new, private, not-for-profit organization created to oversee and manage the critical Internet identifiers, the Internet Corporation for Assigned Names and Numbers (ICANN).

For as the WIPO Advisory Committee was meeting in late 1998 and early 1999, groups were trying to organize a new organization to manage and oversee the critical Internet identifiers, and meet the US Government's requirements set out in the White Paper.

Different groups came forward to share ideas and proposed bylaws with the Department of Commerce, and ultimately NTIA chose the proposal of Jones Day, the law firm that represented Dr. Jon Postel until his untimely death in October 1998. [54]

Jones Day, then the biggest law firm in the world, put forward ideas for the Articles of Incorporation and Bylaws of the Internet Corporation for Assigned Names and Numbers – a name suggested by Network Solutions' President Don Telage because he liked the positive acronym "ICANN."

The infant ICANN quickly signed a Memorandum of Understanding with the Department of Commerce on November 25, 1998, [55] and ICANN began to plan its first public meetings.

54 Dr. Jon Postel died at the age of 55, according to the Los Angeles Times, October, 18, 1998, https://www.latimes.com/archives/la-xpm-1998-oct-18-me-33857-story.html

55 ICANN's Major Agreements and Related Reports, https://www.icann.org/resources/pages/agreements-en

A. Berlin, May 1999

At the time, ICANN began its still-continuing practice of free and open public meetings (if you can get there, you can participate), and meetings were beginning. There was a small organizing meeting in Singapore in early 1999, and a larger meeting in May 1999 in Berlin, a city still uniting after the fall of the wall. We met at an old and elegant hotel, a few hundred people, and most of the constituencies came together.

This was the age of the Domain Name Supporting Organization – with both generic top level domains ("gTLDs") and country code supporting organizations ("ccTLDs") under one roof, which would quickly change to be two different support organizations, and constituencies. Since there was only gTLD registrant/registrar – Network Solutions – most of the work of organizing fell to the Intellectual Property Constituency, the Business Constituency, the Internet Service Providers Constituency, and the Noncommercial Users Constituency.

Most groups formed quickly, but the Noncommercial Users Constituency was much more diverse and needed more time to come together. We did not finish our charter process in Berlin, unlike the other group, and this delay was almost disastrous.

B. WIPO delivered its domain name dispute policy to the infant ICANN, and after with only a month and a half review, Working Group A accepted it, largely unchanged.

Nowadays, the creation of new policies in ICANN, and even the review of old ones, take years. We carefully sit down with diverse stakeholders at the table, gather data, review rules, and debate revisions. But the rules of the Domain Names Supporting Organization (DNSO) for policy development did not then exist (and GNSO did not yet exist), so there were no rules or guidelines for review or acceptance.

WIPO delivered its Final Report on the First WIPO Internet Domain Name Process to ICANN in April 1999. [56] The ICANN Board sent it to the DNSO which delivered it to the hastily-formed DNSO

56 WIPO Internet Domain Name Process, Final Report of the first WIPO Internet Domain Name Process, April 30, 1999, https://www.wipo.int/amc/en/processes/process1/report/index.html

Working Group A, and delivered it into the loving arms of Jonathan Cohen, Intellectual Property Constituency co-founder and Working Group A Co-Chair.

Cohen was Senior, Managing Partner of the Shapiro Cohen Group of Intellectual Property Practices, based in Canada, and with clients around the world. He was at the time, the Intellectual Property Constituency's first president. [57]

Despite calls to slow down the review to a reasonable rate, and many emails seeking to protect registrants (present and future), and analyses of the unfairness and imbalance still present in the proposed WIPO policy, this review was conducted entirely by email between meetings and before the final formation of all constituencies.

I was on Working Group A and it seemed like a "steam roll" to accept the WIPO proposals, in full, as quickly as possible. It was a time before we used email and group phone calls to negotiate policy – still done in person in those days – and thus very difficult to make points and be heard.

After three weeks of discussion and a quick comment period, the chairs of Working Group A proposed accepting the WIPO policy for "cybersquatting" and asked WIPO to tweak a few procedural rules. Today it would take years to properly create and review a substantive policy of this nature, and an ICANN Working Group would know that the responsibility to make clear, substantive changes rests with the Working Group/Policy Development Process Committee members.

On August 3, 1999, the chairs of Working Group A send the WG-A Final Report to the ICANN Board[58]…the Noncommercial users Constituency did not yet even exist.

57 Jonathan Cohen, ICANN Resources, https://www.icann.org/resources/pages/jonathan-cohen-2014-05-23-en

58 WG-A Final Report to ICANN Board, August 3, 1999, http://www.dnso.org/dnso/notes/19990804.NCwga-to-ICANN.html#aaa

C. ICANN Meeting, Santiago, Chile, August 23-26, 1999: ICANN Board reviews the WIPO Domain Name Dispute Policy and Working Group A's recommendations for WIPO to make small revisions, and takes a different direction.

By now, I helped organize a new voice for noncommercial users calling on an old organization. The Association of Computing Machinery (ACM), the first group for programmers and later professors of computer science and founded in 1947, believed in the ethics and best users of the technologies it helped to create (and had been founded by the earliest modern computer pioneers, including several of the ENIAC Programmers, whose story I later wrote in my book, Proving Ground). [59]

I was a member of ACM and appointed the Executive Committee of USACM, ACM's public policy committee. I asked USACM co-founder and then-ACM President Dr. Barbara Simons if ACM would help us organize the noncommercial voice of ICANN and seek a better and more balanced domain name dispute policy. She and ACM understood the importance – and together we applied for a grant from the Ford Foundation to pay for my time and travels (which we quickly received).

1. Traveling to Santiago in August 1999

As I traveled to Santiago in August 1999, I held two documents in hand— first, the completed charter of the Noncommercial Users Constituency (now well discussed online) and second, the resolution to stop adoption of the WIPO domain name dispute policy until there were clear additional protections in the substantive and procedural rules for registrants.

These were not requests for WIPO, but to the ICANN Board and ICANN Community now responsible for the domain name dispute policy they would soon adopt.

Our charter meeting of the Noncommercial Users Constituency (NCUC) went well. It was held in a classroom of the University of Chile, in Santiago (our host), with international

59 Proving Ground: The Untold Story of the Six Women Who Programmed the World's First Modern Computer, Kathy Kleiman, Grand Central Publishing (2022).

groups, including CGI.BR, American Library Association, Association for Computing Machinery, professors and students.

We soon adopted our charter and cheered. Then I shared the deep problems of the domain name dispute rules proposed by WIPO and the too-fast review and adoption by Working Group A. Everyone was deeply concerned about long term problems of adopting a deeply imbalanced and unfair dispute policy.

Among other problems, we talked about the nearly impossible task of proving "good faith" under the proposed new rules for these future arbitrations. For WIPO had proposed a standard of review that required a complaining trademark owner not to prove the traditional legal trademark standard of "infringement," but "bad faith."

WIPO clearly laid out, and Jonathan Cohen and Working Group A embraced, what a trademark owner must prove in their complaint, namely three elements:

> "171. The definition of abusive registration that we recommend be applied in the administrative procedure is as follows:
> (1) The registration of a domain name shall be considered to be abusive when all of the following conditions are met:
> (i) the domain name is identical or misleadingly similar to a trade or service mark in which the complainant has rights; and
> (ii) the holder of the domain name has no rights or legitimate interests in respect of the domain name; and
> (iii) the domain name has been registered and is used in bad faith. [60]

Further, WIPO was very clear in sharing examples for the trademark owners (soon to be called "complainants") and arbitrators (soon to be called "panelists") in examples of bad faith, namely:

> (2) For the purposes of paragraph (1)(iii), the following, in particular, shall be evidence of the registration and use of a domain name in bad faith:
> (a) an offer to sell, rent or otherwise transfer the domain name to the owner of the trade or service mark, or to a competitor of the owner of the trade or service mark, for valuable

60 Paragraph 171, The definition of abusive registration, https://www.wipo.int/amc/en/processes/process1/report/finalreport.html

consideration; or
(b) an attempt to attract, for financial gain, Internet users to the domain name holder's website or other on-line location, by creating confusion with the trade or service mark of the complainant; or
(c) the registration of the domain name in order to prevent the owner of the trade or service mark from reflecting the mark in a corresponding domain name, provided that a pattern of such conduct has been established on the part of the domain name holder; or
(d) the registration of the domain name in order to disrupt the business of a competitor.

But what constitutes good faith registration? How could a registrant accused of being a cybersquatter, and bad faith registration, and had legitimate noncommercial and commercial domain names for that purpose prove their innocence?

To this most vulnerable group, the group most likely to be unrepresented by attorneys, WIPO provided no clear path to proving "good faith" registration to the Panelists.

Our resolution to stop the new domain name dispute policy until there were clear protections for registrants passed easily.

Alas, ICANN's initial draft of the domain name dispute policy was badly unbalanced and procedurally unfair – written largely by people who envisioned themselves only on one side of a case – bringing the complaint and seizing the domain name (laws, regulations and policies are only fair if you can envision yourself on both sides, having to prosecute and defend).

2. Using the Public Forum

What to do next? Then and now ICANN has a remarkable feature: the Public Forum.

In Santiago, we took our concerns to the Public Forum that took place at the end of the ICANN meeting and NCUC converged on this meeting to share our concerns. Three minutes is not much time to speak, so our newly-minted NCUC members took turns at the microphone sharing our concerns about the domain name dispute policy and the disastrous consequences for registrants around the world, and speech online.

As the leader and key researcher at the meeting, I went to

the microphone again and again to outline the problems.

Together we laid out key issues, including.

- Shouldn't groups and individuals using domain names for educational, research, personal and political speech be protected, as they were for years on the NSF Internet?

- How could we create clear rules to protect small non-profit organizations and entrepreneurs coming online to share their information, products and services?

- Do not all registrants, and particularly registrants who do not speak English and have never heard of this proceeding, have sufficient time to research the notice of complaint, find support to prepare a response, and sufficient time to defend their domain name?

I was very proud of our group.

3. Our Concerns made sense to the Board and to Jeri Clausing of the New York Times.

Fortunately, the Board listened. The Board members came from an array of background and the concerns for the future that we raised seemed to resonate.

Our concerns also made sense to a young journalist, Jerri Clausing, who was covering the ICANN meeting in person for the New York Times. She talked with me earlier in the week, and then covered the public forum. See, for example, Internet Board Opens Chile Meeting Amid Protests, New York Times, August 24, 1999. [61] (I learned from my parents, avid readers of the New York Times, that my quotes and our concerns appeared several times in the New York Times that week as Jerri sent her stories back to the editors).

61 https://archive.nytimes.com/www.nytimes.com/library/tech/99/08/cyber/articles/25domain.html

D. The Board called for substantial change and balancing.

In the end, at its meeting on August 26, 1999, the ICANN Board approved a domain name dispute policy in theory, but with requirements for significantly more fairness and balance in substantive and procedure.

Specifically, the Board resolution stated [62]:

> 1. The registrars' Model Dispute Resolution Policy should be used as a starting point;…
> 3. In addition to the factors mentioned in paragraph 171(2) of the WIPO report, the following should be considered in determining whether a domain name was registered in bad faith:
> (a) Whether the domain name holder is making a legitimate noncommercial or fair use of the mark, without intent to misleadingly divert consumers for commercial gain or to tarnish the mark
> (b) Whether the domain name holder (including individuals, businesses, and other organizations) is commonly known by the domain name, even if the holder has acquired no trademark or service mark rights; and
> (c) Whether, in seeking payment for transfer of the domain name, the domain name holder has limited its request for payment to its out-of-pocket costs.
> 4. There should be a general parity between the appeal rights of complainants and domain name holders.
> 5. The dispute policy should seek to define and minimize reverse domain name hijacking…"

In addition, the Board took responsibility for the final version of the domain name dispute policy, not handing it back to WIPO, but to a new group that it would appoint:

"The President or his delegate should convene a small drafting committee including persons selected by him to express views and consider the interests of the registrar, non-commercial, individual, intellectual property, and business interests…"

62 https://archive.icann.org/en/meetings/santiago/santiago-resolutions.htm

VII. The ICANN Board Created a New Group: The Final Drafting Team

A month later, in September 1999, the ICANN Board created a small drafting team[63]. They called it "implementation language," but tasked the new group with much broader work – to "consider the interests of registrar, non-commercial, [and] individual" as well as intellectual property and business

A small group was assembled and we all agreed to serve:

Name	Groups
Kathryn A. Kleiman	ACM's Internet Governance Committee and the Non-Commercial Domain Name Holders' Constituency
A. Michael Froomkin	University of Miami School of Law and dissenting voice on WIPO's Panel of Experts)
Rita A. Rodin	The large law firm of Skadden, Arps, Slate, Meagher & Flom, representing America Online and the new Registrars Constituency
Steven J. Metalitz	General Counsel for the International Intellectual Property Alliance and member Intellectual Property Constituency
J. Scott Evans	Adams Law Firm P.A. and Chair of the International Trademark Association's Domain Name System Subcommittee

We had a lot of work to do. Despite the clear direction from the ICANN Board for change, Metalitz and Evans opposed most of it. But with Louis Touton, ICANN's only staff member at the time (former attorney with Jones Day), I spent hours and days working through the language of a new section to lay out registrant rights and responses, expand the time for response and improve notice.

I also pursued the golden ring – recognition that trademark owners

63 Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy, Posted: September 29, 1999, https://archive.icann.org/en/udrp/staff-report-29sept99.htm

and their attorneys might also could act in bad faith and bring complaints to harass, intimidate and steal domain names from good faith registration. In the domain name work, this form of bullying was called "Reverse Domain Name Hijacking," and we wanted this bad faith called out by the Panels.

There were long fights and hard days; we met in person at least once and then had many conference calls and emails. Finally, we agreed on significant new policy terms, and slightly improved procedural ones:

We proposed the addition of Section 4(c) to clearly lay some examples of protected and allowable registration of domain names, as we had now been discussing for years:

> "Section 4(c). How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint" [64]
> "(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or
> (ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or
> (iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue."

I consider this section to be my most important addition to the new policy.

A. Other changes to the policy

We also achieved "parity of appeal," allowing both registrants and trademark owners to appeal a decision to court that they thought was unfair (in reality, there are some countries that have the laws to allow these appeals, and some that do not).

Further, we placed with the policy recognition that bad faith can take place on both sides, and that trademark owners can bring a complaint in bad faith, to harass or intimidate a registrant, or to steal

64 Uniform Domain Name Dispute Resolution Policy (1999), https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-25-02-2012-en

their domain name. This act was worthy of being identified and called out. At the time, we were told no decision maker would ever use it, but of course, they can and do.

B. The New Policy Goes in Effect

The revised policy went into effect in October 24, 1999 – the first consensus policy of ICANN – with its new name, the Uniform Dispute Resolution Policy or "UDRP." At the time, there were ICANN-approved UDRP Providers. Later and for years, only WIPO would be ICANN's approved place to submit UDRP complaints. Over time, the list has grown to five, and the forum is chosen by the trademark owner.

We hope that the upcoming review of the UDRP will look at the issue of forum shopping (choosing a Provider in hopes of obtaining a favorable outcome) closely. Fundamental fairness requires us to have forums that treat both parties equally.

With that, on October 24, 1999, the UDRP went into effect and before the end of the year, WIPO read its first cases (for UDRP is a fully virtual forum and all of the proceedings are conducted online via filings and no hearings. It was the world's first fully-virtual proceeding.

VIII. Our Work is Not Yet Done

After 26 years of UDRP decisions, some people like it and some people do not. Many say that the UDRP succeeded in achieving balance in its substantive rules, and I would respond that we worked very hard to do that.

Certainly, the UDRP is faster and cheaper than court, and that was a key goal for the Department of Commerce and for ICANN. But is it fairer than court? The answer is no, in large part because the UDRP strips away personal jurisdiction – the right to be sued in your own court, and to only be stripped of your liberty or property in a forum with which you have direct ties – such as a court near your homes, speaking your language, with customs and notices you know.

Only trademark owners and their attorneys (now appearing in case after UDRP case) know the UDRP proceedings. For nearly every registrant involved in these proceedings, the existence of these rules is new as is the forum – WIPO or The Forum or the other newer UDRP Providers. The rules, policies, procedures, even language may be unknown to the registrant, as many registrants around the world are doing the domain name system from non-English speaking parts of the world (a growth pattern that ICANN supports and encourages).

As we study the data of the UDRP, we see registrant after registrant trying to communicate with WIPO and not appearing to receive useful guidance. [65] Over the last 25 years, WIPO has spent many days and conferences teaching trademark owners about the UDRP, but has it held even one conference to teach registrants how to respond to UDRP complaints?

If we seek equity and parity, it would seem fair for the UDRP forums (the "Providers") to provide detailed educational materials, teaching programs, and review of submissions and useful edits for both trademark owners and registrants.

Further, if these valuable street signs must be removed in a distant virtual forum, would it not be fair to ensure representation for both sides, including good faith registrants?

While ICANN's UDRP currently does not provide counsel for registrants, the Chilean country code, .CL does. Dismayed at watching entrepreneurs, small businesses, small organizations and individuals lose valuable domain names in the .CL UDRP proceedings (a localized version of the domain name dispute process applying only to domain names in .CL), General Council Margarita Valdés of NIC Chile asked leading law schools in her country to work with students to defend registrants, and they set up clinics and used law school time to do so. These registrants win far more cases than unrepresented registrants in the UDRP proceedings.

A. In the upcoming UDRP review, let's look closely at substance and procedure

ICANN soon will look at the UDRP again. For the first time in 25 years, we will have a review under ICANN's current policy development process. We know how to do this now (having in 2020 completed extensive reviews of the Trademark Clearinghouse and Uniform Rapid Suspension in a four-year process I co-chaired).

Let's take a hard look at the fairness and balance of the substantive and procedural of the UDRP. Further, let's closely review the additional rules adopted by the Providers – and never examined by the ICANN Community process: Are they fair, balanced and just?

B. Additional issues we should consider

Additional issues we should consider include:

1) Response time: While trademark owners and their attorneys can

65 Author is currently co-leading a project surveying all 2024 UDRP decisions.

spend many days preparing their filings, registrants have a very limited time to respond. Can we expand the time for a response – or encourage requests for extension that receive close attention and likely grant?

2) Notice: Are Registrants receiving "actual notice" of the proceedings or are their emails going into the ether as email systems increasingly block emails from groups with no known relationship with the registrant? Are there other ways to ensure that the Registrant receives notice – perhaps with an additional notice from the Registrar (with whom the Registrant has a trusted relationship).

3) Educational materials: Many rounds of revised materials exist for trademark owners and their attorneys, but how much time has gone into creating readable, usable educational materials for registrants? Can we do better with focus groups and input from registrant groups and attorneys?

4) Languages: Are notices and complaints being provided in the language of the registration agreements and the language of the registrants?

5) Registrar education: Some registrars believe they cannot talk with their registrants once a UDRP is filed, yet their registrars are a good first place for registrants to turn – particularly when (without notice) their domain names are frozen by their registrars. Can we help Registrars to know that Registrants may need their help and support, as well as their explanation?

6) Providers: Are the Panelists fair and impartial? There appear to be questions here as some well-known trademark attorneys are appointed again and again as panelists, while equally well-trained registrant attorneys are never allowed to be.

7) As above, how do we help more registrants to be represented before they lose their valuable domains and with them their websites, emails and listservs?

Conclusion

Freedom of expression in Article 19 of the UN Declaration of Human Rights and free speech in the US Constitution's First Amendments are rights we guarantee to all peoples. Removal of that speech requires fairness and due process.

For the Internet is "the most participatory form of mass speech yet developed" and since 1999 has grown from about 50 million people to

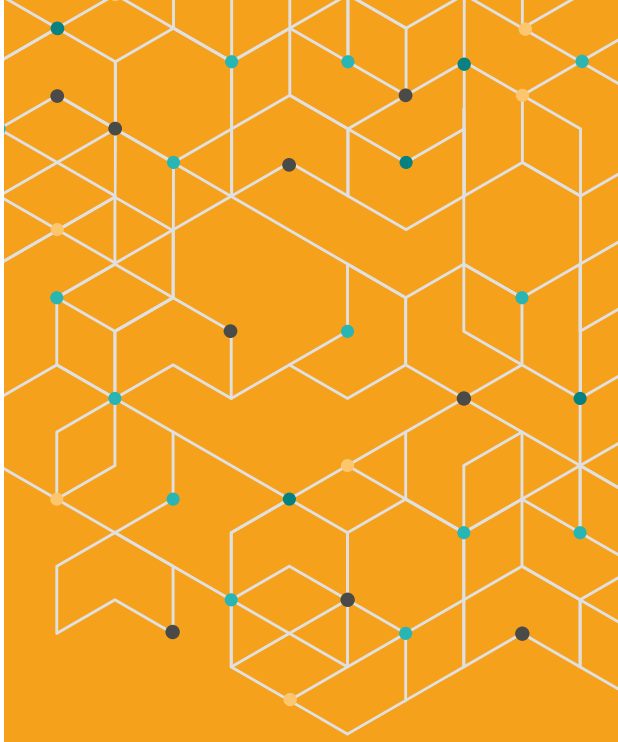
over 5 billion people – many with ideas and organizations, noncommercial groups and growing companies.

The interest in domain names continues to grow as we introduce new top level domains in many languages, and as the desire to control one's own content, email addresses and listservs grows. With over 1300 generic top level domains, from .COM and .NET to .VIP, .TECH and .HORSE, there should be room for everyone and, indeed, 200 million domain names are now registered.

I look forward to a full and fair review of the UDRP to ensure that every registrant can share their speech, their ideas, and their services. The future of our shared speech depends on it.

Epilogue

In 2018, the Internet Commerce Association awarded me the Lonnie Borck Memorial Award in memory of a well-loved member of their group. The plaque reads: "in recognition of the enormous efforts she has made for over 20 years advocating on behalf of domain name registrants, particularly at ICANN." I was very moved and honored, and surprised anyone remembered these events of early domain name policy.



registro.br nic.br cgi.br