THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY: A CHEAPER WAY TO HIJACK DOMAIN NAMES AND SUPPRESS CRITICS

Keith Blackman*

TABLE OF CONTENTS

I. INTRODUCTION ....................................212

II. BACKGROUND .....................................213
   A. Trademark Infringement by Confusion ............215
   B. Trademark Dilution .............................216
   C. Anticybersquatting Consumer Protection Act ....220

III. DEVELOPMENT OF THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY ................................221
   A. Network Solutions, Inc. ..........................221
   B. Uniform Domain Name Dispute Resolution Policy ......223
      1. Development of the Uniform Domain Name Dispute Resolution Policy .....................223
      2. Proper Scope of the Uniform Policy ................230

IV. ANALYSIS OF THE UNIFORM POLICY AND ITS APPLICATION . 231
   A. Reverse Domain Name Hijacking ..................233
   B. Tarnishment and Free Speech .....................236
      1. Applicability of the Constitution to the Uniform Policy .................................237
      2. The Suppression of Legitimate Criticism by Dispute Resolution Panels ..............243

V. <TRADEMARK>sucks.com: A CASE STUDY ..............246

VI. CONCLUSION ......................................255

* Associate (not yet admitted to practice) at Debevoise & Plimpton, New York, N.Y.; J.D., cum laude, Harvard Law School. The views expressed in this Note are the author’s own. The author wishes to thank Professor William W. Fisher III of Harvard Law School for his insight and encouragement in preparing this Note. He would also like to thank his wife Rebecca for her ceaseless love and support.
I. INTRODUCTION

Until last year, U.S. trademark owners seeking to assert their rights on the Internet were forced to litigate in a court under the often inapplicable theories of trademark infringement or trademark dilution. Although Congress sought to facilitate legitimate claims of trademark infringement by passing the Anticybersquatting Consumer Protection Act (“ACPA”), the new law did not provide a speedy, inexpensive method of securing the transfer of a domain name from an infringing party.

In October 1999, after receiving authority from the United States Department of Commerce to control domain name registration, the Internet Corporation for Assigned Names and Numbers (“ICANN”) instituted a Uniform Domain Name Dispute Resolution Policy (“Uniform Policy”). This agreement provided an alternative to litigation for abusive cases of cybersquatting (where a speculator registers domain names that are similar or identical to trademarks and seeks to sell these names to the mark owners) and cyberpiracy (where the registrant intentionally diverts customers from a competitor’s website for commercial gain). It left cases where two parties had legitimate competing claims to a domain name for judicial resolution.

While the Uniform Policy represents an improvement over costly litigation and the previous dispute policy implemented by Network Solutions Inc., it can also be used to facilitate reverse domain name hijacking — where a trademark owner asserts overextensive trademark rights over a domain name — and to impinge upon free speech. This Note illustrates the ways in which the Uniform Policy can be used, and has already been used, to enable mark owners to expand their trademark rights on the Internet in ways that are impermissible under United States law.

In Part II, this Note summarizes existing trademark law as it has been applied to the Internet. It defines the boundaries of the law before the passage of the ACPA and attempts to predict the changes wrought by the new law. Part III provides a history of the Uniform Policy and demonstrates its superiority over the previous dispute policy, emphasizing the proper and limited application of the Uniform Policy. Finally, Part IV demonstrates how the Policy exceeds its authority both in its language and — more particularly — in its application by administrative panels. In their decisions, these panels usurp the role of the judiciary by deciding cases properly left to the courts, expand the legal rights of trademark owners by facilitating reverse domain name hijacking, and encroach upon the First Amendment rights of domain name registrants.
II. BACKGROUND

Domain names — or the alphanumeric identifiers for websites — are exclusive. In other words, two website owners cannot have identical domain names. For this reason, while two non-competing users of a trademark can legally register the same mark, these companies are not able to identify their sites with an identical incorporation of the mark into a domain name. In fact, even if they used similar domain names, some customers would end up in the wrong place notwithstanding the fact that the two companies sold different goods and operated in different states or countries. The desire to stake a claim on the borderless Internet has led to conflict in situations where there used to be (relatively) peaceful coexistence.

The unique aspects of trademark use on the Internet have led companies to adopt strategies to get the most value from their trademarks. For example, since customers tend to type “<company>.com” when seeking a particular company’s web page, there is often a race among businesses to register the most intuitive domain name for their firms.

Attempts by companies to utilize their trademarks as domain names have been threatened by two activities. First, “cyberpirates” obtain

1. For a brief background to domain names, see J.TOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:75 (4th ed. 1998).
2. Judge Calabresi explains this phenomenon in SPORTY’S FARM v. SPORTSMAN’S Mkt., 202 F.3d 489 (2d Cir. 2000).
3. Although this Note distinguishes between “cyberpiracy” and “cybersquatting,” some sources equate the two terms to include both registering domain names with an intent to sell them and registering with an intent to divert customers. See, e.g., H.R. REP. NO. 106-412, at 9 (1999) (“Cyberpiracy (or cybersquatting) consists of registering, trafficking in, or using domain names (Internet addresses) that are identical or confusingly similar to trademarks with the bad-faith intent to profit from the goodwill of the trademarks.”). I will follow WIPO’s nomenclature, which denotes as cyberpiracy violations of intellectual property laws in the content of websites, while cybersquatting refers to abusive domain name registrations. See WIPO, Final Report of the WIPO Internet Domain Name Process, “The Management of Internet Names and Addresses:
domain names in order to divert customers from a trademark owner’s site to their own, thereby profiting off the mark’s goodwill. Cyberpirates benefit by either confusing customers as to the source of the goods or services sold or by generating advertising revenue from drawing additional customers.

A second threat has come from “cybersquatting.” A cybersquatter is a “speculator who knowingly reserves a trademark as a domain name merely to sell it for a profit.” It has traditionally been difficult for companies to combat this practice in court because it is often easier to pay off the cybersquatter rather than pursue a lawsuit.

Until 1999, trademark owners needed to invoke the provisions of the Lanham Act in order to protect their trademark rights from these threats. Mark owners would generally bring claims under either a trademark infringement or trademark dilution theory. For some cases, the traditional legal framework was easily applied to the Internet scenario; for many others, however, courts artificially extended settled principles

---


Revenue on the web is still driven largely by advertising, and advertising is based on traffic (“hits”) to the site, rather than sales from the site. Thus, many “cyberpirates” try to lure this traffic by registering domains that are identical or similar to popular trademarks. Misspelling Nike as nikee.com does indeed draw consumers and generate more hits.

Id. at 12.


Regardless of the ultimate outcome of litigation, trademark owners must expend significant resources and endure the inevitable delay associated with bringing a civil action in order to validate their rights. Many companies simply choose to pay extortionate prices to [cybersquatters] in order to rid themselves of a potentially damaging headache with an uncertain outcome. For example, Gateway recently paid $100,000 to a [cybersquatter] who had placed pornographic images to the Web site ‘www.gateway20000.’

Id. at 6.

8. Although unfair competition under 15 U.S.C. § 1125(a) is also asserted by plaintiffs in abusive domain name registration suits, the “test for unfair competition under Section 1125(a) is essentially the same as that for trademark infringement under Section 1114, namely whether there is a likelihood of confusion between the marks.” Jews for Jesus v. Brodsky, 993 F. Supp. 282, 309 (D.N.J. 1998).

---

Pagination incorrect - not for citation
to address the unique problems raised by abusive domain name registration. In 1999, Congress responded to the requests of trademark owners to pass a law more specifically applicable to their needs. The result was the ACPA.9

This Section briefly summarizes the development of traditional trademark law as it pertains to domain names. It points out some of the problems of applying this law to cyberspace and then analyzes how the passage of the ACPA was seen as an effort to solve these problems.

### A. Trademark Infringement by Confusion

A traditional trademark infringement claim is only applicable when the alleged infringer causes customer confusion as to the source of goods or services.10 This action is most effective against cyberpiracy, where the registrant uses a confusing domain name to lure customers to his or her site for commercial gain.

However, it is difficult to fit cybersquatting under this definition of trademark infringement. Although courts use numerous tests to determine whether confusion exists,11 most instances of cybersquatting do not confuse consumers to any appreciable degree. A speculator who registers a domain name for the purpose of selling it to the trademark

---


   Any person who shall, without the consent of the registrant — (a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or (b) reproduce, counterfeit, copy, or colorably imitate a registered mark and apply such reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive, shall be liable in a civil action by the registrant for the remedies hereinafter provided. Under subsection (b) hereof, the registrant shall not be entitled to recover profits or damages unless the acts have been committed with knowledge that such imitation is intended to be used to cause confusion, or to cause mistake, or to deceive.

Id. (emphasis added).

11. The classic test considers the eight “Polaroid factors”: the strength of plaintiff’s mark; the degree of similarity between plaintiff’s and defendant’s marks; the proximity of the products or services; the likelihood plaintiff will bridge the gap; evidence of actual confusion; defendant’s good faith in adopting the mark; the quality of defendant’s product or service; and the sophistication of the buyers. See Polaroid v. Polarad Elec. Corp., 287 F.2d 492, 495 (2d Cir. 1961), cert. denied, 368 U.S. 820 (1961).
holder often does not attempt to deceive customers who access that website.12 Moreover, since the registrant often does not post anything at all to the site, the complaining mark owner is unable to demonstrate that the defendant used the mark in commerce, as required by trademark infringement law. In fact, the registrant often does not post anything at all to the site.

B. Trademark Dilution

Due to the difficulty of proving trademark infringement under 15 U.S.C. § 1114(1), mark owners typically sue under the Federal Trademark Dilution Act (“FTDA”).13 The dilution statute provides for an injunction “against another person’s commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.”14 Thus, to sue under the dilution statute, plaintiffs do not need to prove the presence of competition between the parties or any likelihood of consumer confusion, mistake, or deception.15 The legislative history of the Act indicates that Congress meant for the Federal Trademark Dilution Act to apply to cyberpiracy and cybersquatting,16 and it has accordingly been used for that purpose.17
The trademark dilution law does not perfectly fit all instances of abusive domain name registration, however. First, some activities do not fit into either of the traditional theories of trademark dilution: blurring or tarnishment. “‘Blurring’ is the unauthorized use of a mark on dissimilar products or for dissimilar services that may cause the mark to cease functioning as a unique identifier of the goods and/or services of the owner of the mark.”18 The Northern District of Illinois applied the “blurring” rationale in *Intermatic, Inc. v. Toeppen*19 when it found that the defendant, a domain name speculator, diluted the plaintiff’s mark. The court noted, “The harm caused by dilution is, for example, that the distinctiveness of the name [Intermatic] and the favorable association that accrued to it by virtue of [Intermatic’s] commercial success would be undermined by the use of similar names in connection with other non-competing and non-confusing products.”20 On the other hand, “[t]arnishment occurs where a mark becomes consciously or unconsciously linked with poor quality, unsavory, or unwholesome goods or services.”21 For example, the Western District of Washington granted a preliminary injunction preventing a sexually explicit Internet site from using the domain name “candyland.com,” (a trademark used in connection with a children’s board game) due to the plaintiff’s likelihood of prevailing on its dilution claims.22 The court was clearly concerned that the adult Internet site would tarnish the toy company’s mark.

While abusive domain name registrations often either blur or tarnish the mark owner’s trademark, there are many cases where neither theory applies. For example, when a cybersquatter registers a trademarked domain name and seeks to sell the name to the mark holder without posting anything to that Internet site, no blurring or tarnishment occurs. However, courts have not been troubled by an inability to fit dilution into one of the traditional theories. In *Panavision International v. Toeppen*, the Ninth Circuit held that “[t]o find dilution, a court need not rely on the traditional definitions such as ‘blurring’ and ‘tarnishment.’”23 Instead, the Panavision court based its finding of dilution on the fact that the defendant’s conduct “diminished ‘the capacity of the Panavision

(affirming district court’s finding that defendant’s speculation activities constituted trademark dilution). As one commentator has noted, “[t]he Federal Trademark Dilution Act is probably the strongest weapon against unauthorized use of a trademark in a domain name by parties with no colorable claim to the mark.” Landau, supra note 12, at 478.
marks to identify and distinguish Panavision’s goods and services on the Internet." A commentator has labeled this rationale “dilution by elimination.”

A second problem with applying dilution law to cybersquatting and cyberpiracy is that a trademark dilution claim is only available to owners of “famous” marks. It is speculated that, if cybersquatting cases continue to be litigated under the dilution statute, the “famousness” restriction will result in either lowered protection for owners of non-famous marks or an artificial extension of the definition of “famous” by the courts. In cybersquatting cases, courts have tended to interpret the “famousness” requirement broadly. For example, the Hasbro court found that the plaintiff would likely win its dilution suit without considering whether Hasbro’s “CANDY LAND” mark could be considered “famous.”

A final difficulty in applying the dilution statute to many domain name cases is the “commercial use in commerce” requirement. Courts have held that “non-commercial use of a domain name that impedes a trademark owner’s use of that domain name does not constitute dilution.” However, the “use in commerce” requirement has not limited the application of the statute to cases where products are bought and sold. In a notable example, a New Jersey district court found that the defendant engaged in commerce when he used the plaintiff’s trademark as the domain name for a website that protested against the plaintiff organization. The court found that the defendant met the “use
in commerce” requirement by (1) “hyperlinking” to an organization that sells merchandise and (2) harming the plaintiff organization commercially.32 A similar extension of the “commercial use” requirement has been seen in cybersquatting cases. In Panavision,33 the Ninth Circuit affirmed the district court’s finding that, even though “mere registration” of a domain name does not constitute commercial use, selling these names to trademark owners is such a use. These activities stretch the definition of “commercial use” and demonstrate the willingness of courts to find dilution in cybersquatting cases.34

C. Anticybersquatting Consumer Protection Act

Despite the success that trademark owners have had in challenging cyberpirates and cybersquatters under traditional claims of infringement and dilution, Congress passed the ACPA35 in 1999 to target certain “bad faith” domain name registrations more specifically and to avoid reliance on an often inapplicable dilution claim. In the first case decided under the ACPA, Judge Calabresi recognized this justification for the new law, opining, “[W]e think it is clear that the new law was adopted specifically to provide courts with a preferable alternative to stretching federal dilution law when dealing with cybersquatting cases.”36

The new law establishes civil liability when a person has a bad faith intent to profit from the registration, traffic, or use of a domain name that is identical or confusingly similar to a distinctive trademark, or is identical, confusingly similar to, or dilutive of a famous mark.37 Like the dilution statute, the ACPA does not require competition38 or customer confusion.39 It expands the theoretical reach of the Lanham Act by

32. See id. at 308.
33. 141 F.3d 1316, 1324 (9th Cir. 1998).
34. See Golinveaux, supra note 6, at 647–48. “Mere reservation of a domain name which contains another’s trademark, with no additional use of either the trademark or Web site, should not be considered dilution, even in the case of cybersquatting. There is no commercial use in commerce as required by the Lanham Act’s anti-dilution provision.” Id. at 671.
38. The Act applies “without regard to the goods or services of the parties.” Id. § 1125(d)(1)(A).
39. The Act applies even if the domain name is merely “dilutive” of a trademark. Id. § 1125(d)(1)(A)(ii)(II).
extending beyond “famous” marks; however, it narrows the scope of “commercial use” to apply only to “bad-faith intent to profit.”

The Act then lists nine factors for courts to apply in order to determine whether “bad-faith intent” exists:

- Whether the domain name holder has any trademark or other intellectual property rights in the domain name;
- The extent to which the domain name consists of the holder’s name;
- The domain name holder’s prior use of the domain name in connection with the bona fide offering of any goods or services;
- The domain name holder’s bona fide noncommercial or fair use of the mark on the website;
- Whether the domain name holder intended to divert consumers from the mark owner’s site for commercial gain or to tarnish the mark;
- Whether the holder offered to sell the domain name to the mark owner or a third party for financial gain, without intending to use the domain name in the bona fide offering of any goods or services; or a pattern of such conduct;
- The provision of material and misleading false contact information;
- The holder’s registration or acquisition of multiple domain names that are identical or confusingly similar to other distinctive marks;
- Whether the mark is distinctive or famous within the meaning of the FTDA.

---

41. See id. § 1125(d)(1)(A)(i).
42. See id. § 1125(d)(1)(B)(i).
Regardless of whether these conditions are met, there will be no liability if the court finds that the domain name holder reasonably believed that the use of the domain name was a fair use or otherwise lawful.\footnote{See id. § 1125(d)(1)(B)(ii).}

III. DEVELOPMENT OF THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY

A. Network Solutions, Inc.

In 1991, the National Science Foundation gave a private company, Network Solutions, Inc. (“NSI”), a monopoly in registering domain names on the Internet.\footnote{See Andrew R. Basile, \textit{Recent Developments: Intellectual Property Law and the Internet}, 584 PLI/PAT 293, 299 (1999). Basile provides an excellent background of intellectual property law on the Internet, as well as a summary of the major developments from June 1998 to June 1999.} By 1995, NSI had created a dispute resolution policy to insulate itself from potential litigation.\footnote{See id. at 300. Future cases established that NSI had no obligation to screen domain name registrations for potential trademark violations. See Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949 (C.D. Cal. 1997); \textit{see also} Acad. of Motion Picture Arts & Scis. v. Network Solutions, Inc., 55 U.S.P.Q.2d 1463 (C.D. Cal. 1997).}

To invoke the NSI Dispute Policy, the complainant would have to give notice to the registrant that there had been an alleged trademark violation because the “creation date” of the registrant’s domain name registration followed the “effective date” of the complainant’s registration of an identical trademark.\footnote{See Abramson, \textit{supra} note 18, at 32 (containing Revision 03 of Network Solutions Domain Name Dispute Policy (“NSI Policy”)). The final revision of the NSI Policy can be found in \textit{McCarthy}, \textit{supra} note 1, § 25:75.} After NSI received a copy of the complaint, the registrant would have thirty days to prove that he owned a trademark in the contested name.\footnote{See id. at 300. The registrant could avoid having his domain placed on hold by commencing a declaratory action in a court of competent jurisdiction. This way, he could stay online pending a final court decision. See Abramson, \textit{supra} note 18, at 14.} If he could not, NSI would put the domain name on “hold” until a resolution was reached, either between the parties or through litigation.\footnote{See id. para. (d).}

The NSI Dispute Policy was criticized by many because it did not, in fact, resolve the dispute. As the Policy itself stated, “Network Solutions neither acts as arbiter nor provides resolution of disputes between registrants and third party complainants arising out of the registration or use of a domain name.”\footnote{Abramson, \textit{supra} note 18, at 32, paras. 9(c)-(d).} A related problem was that the NSI Policy facilitated “reverse domain name hijacking,” which occurs...
when a trademark owner asserts trademark rights over a domain name even though these rights exceed those afforded to him by law. Reverse domain name hijacking was made possible by the combination of (1) an easy method of placing an alleged infringer’s domain registration on hold and (2) the limited defense available to the registrant, consisting solely of showing that he or she owned a trademark in a mark incorporated in the domain name. In a policy paper known as the “White Paper,” the National Telecommunications and Information Administration (“NTIA”) of the Department of Commerce reported that retaining a system such as NSI’s “would significantly extend trademark holders’ rights beyond what is accorded in the real world.”

In 1999, the U.S. Department of Commerce transferred authority of the domain name registration system to a non-profit organization, the Internet Corporation for Assigned Names and Numbers (“ICANN”). Soon after, ICANN took a more active role in resolving domain name disputes.


51. The transfer of authority from NSI to ICANN had been the primary recommendation of the NTIA’s White Paper. See White Paper, supra note 50; see also McCarthy, supra note 1, § 25:73.1. “ICANN consists of a broad coalition of business leaders, technical advisers, academics, and other Internet users.” Marcelo Halpern & Ajay K. Mehrotra, From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age, 21 U. PA. J. INT’L ECON. L. 523, 547 (2000); see also A. Michael Froomkin, Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, 50 DUKE L.J. 17, 50–93 (2000) (detailing the history of ICANN).
B. Uniform Domain Name Dispute Resolution Policy

1. Development of the Uniform Domain Name Dispute Resolution Policy

In its White Paper, the NTIA requested that the World Intellectual Property Organization ("WIPO") of the United Nations conduct a consultative study on domain name and trademark issues. Among its recommendations to WIPO, the NTIA suggested that a system be adopted whereby domain name registrants, at the time of registration, would agree to and be bound by an alternative dispute resolution system designed to resolve trademark conflicts.

52. A useful outline of the Uniform Policy’s history is available at ICANN’s website. See Timeline for the Formulation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy, at http://www.icann.org/udrp/udrp-schedule.htm (last updated Oct. 17, 2000). For an exhaustive and critical look at ICANN’s history, see Froomkin, supra note 51, at 50–93. Other commentators have outlined the history of ICANN in a more complimentary light. See, e.g., Halpern & Mehrrota, supra note 51, at 546–60; McCarthy, supra note 1, at 25:73.1.

53. See White Paper, supra note 50, at 31,751. WIPO “is one of the sixteen [16] specialized agencies of the United Nations system of organizations”, and “is responsible for the promotion of the protection of intellectual property throughout the world through cooperation among States, and for the administration of various multilateral treaties dealing with the legal and administrative aspects of intellectual property.” What is WIPO, at http://www.wipo.org/eng/dgtext.htm (last visited Nov. 8, 2001).

54. See White Paper, supra note 50, at 31,750–51. The White Paper enumerated four suggestions in the “Trademark Issues” section:

1. Domain registrants pay registration fees at the time of registration or renewal and agree to submit infringing domain names to the authority of a court of law in the jurisdiction in which the registry, registry database, registrar, or the “A” root servers are located.
2. Domain name registrants would agree, at the time of registration or renewal, that in cases involving cyberpiracy or cybersquatting (as opposed to conflicts between legitimate competing rights holders), they would submit to and be bound by alternative dispute resolution systems identified by the new corporation for the purpose of resolving those conflicts. Registries and Registrars should be required to abide by decisions of the ADR system.
3. Domain name registrants would agree, at the time of registration or renewal, to abide by processes adopted by the new corporation that exclude, either pro-actively or retroactively, certain famous trademarks from being used as domain names (in one or more TLDs) except by the designated trademark holder.
4. Nothing in the domain name registration agreement or in the operation of the new corporation should limit the rights that can be asserted by a domain name registrant or trademark owner under national laws.

Id.
WIPO submitted a Final Report to ICANN in April 1999.\(^{55}\) WIPO recommended the adoption of a mandatory dispute resolution procedure to address allegations of cybersquatting.\(^{56}\) Like the White Paper, WIPO’s recommendation called for a minimalist approach, limited to “cases of bad faith, abusive registration of domain names that violate trademark rights (‘cybersquatting,’ in popular terminology).”\(^{57}\) In

---

55. See WIPO Report, supra note 3.
56. See id. ¶¶ 129–244.
57. Id. at vi; see also Halpern & Mehrotra, supra note 51, at 551. The WIPO Report noted that such cybersquatting “was universally condemned throughout the WIPO Process as an indefensible activity that should be suppressed.” WIPO Report, supra note 3, at vi.

The WIPO Report’s definition of “abusive registration” was a precursor to ICANN’s Uniform Policy:

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.

(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 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.

... The cumulative conditions of the first paragraph of the definition make it clear that the behavior of innocent or good faith domain name registrants is not to be considered abusive... Domain name registrations that are justified by legitimate free speech rights or by legitimate non-commercial considerations would likewise not be considered to be abusive. And, good faith disputes between competing right holders or other competing legitimate interests over whether two names were misleadingly similar would not fall within the scope of the procedure.
addition, the Final Report recommended that the administrative procedure be “quick, efficient, cost-effective and conducted to a large extent on-line” and that determinations under it be “limited to orders for the cancellation or transfer of domain name registrations and the allocation of the costs of the procedure (not including attorneys’ fees) against the losing party.”

WIPO’s suggestions were submitted to and revised by the Domain Name Supporting Organization (“DNSO”), a subgroup of ICANN. The DNSO did not alter WIPO’s recommendations in any meaningful way; it urged that ICANN promptly adopt a Uniform Dispute Resolution Policy that “should apply only to bad-faith/abusive domain name registrations (cybersquatting) on a mandatory basis, but without precluding the parties’ ability to litigate the dispute.”

On August 26, 1999, ICANN accepted the DNSO’s recommendation to create a uniform dispute resolution procedure. It called upon a small committee to draft a policy, using as a starting point WIPO’s Final Report, as well as a proposed “Model Dispute Resolution Policy for Voluntary Adoption” created by a group of twenty registrars.

---

WIPO Report, supra note 3, ¶¶ 171–72.

58. WIPO Report, supra note 3, at vi. The WIPO report also recommended a mechanism for reserving domain names identical to famous trademarks for the mark owners. See id. ¶¶ 245–303. At a recent ICANN Board Meeting, the board resolved to ask WIPO for a list of “globally-famous trademarks” to assess whether to reserve domain names for these trademarks on new generic top-level domains. See Preliminary Report of the Meeting of the ICANN Board in Cairo, at http://www.icann.org/minutes/prelimreport-10mar00.htm (Mar. 10, 2000).


60. DNSO Report, supra note 59. While the DNSO recommended that WIPO clarify some of its provisions, it ultimately urged the speedy implementation of WIPO’s Uniform Policy. See id.

61. The members of the drafting committee were chosen because of their legal drafting abilities and because they collectively represented a diversity of viewpoints. See Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy [hereinafter First ICANN Staff Report], at http://www.icann.org/udrp/staff-report-29sept99.htm (Sept. 29, 1999).

62. See Minutes of Meeting of Aug. 26, 1999, at http://www.icann.org/minutes/minutes-26aug99.htm (approved Oct. 24, 1999); see also Model Domain Name Dispute Resolution Policy for Voluntary Adoption by Registrars, at http://www.icann.org/santiago/registrar-dispute-policy.htm (Aug. 20, 1999). The operative section of the proposed Model Dispute Resolution Policy for Voluntary Adoption provided the basis for creating implementation documents for ICANN’s uniform dispute resolution policy.
In September 1999, the first draft of the “implementation
documents,” consisting of a policy and procedural rules, was appended
to an ICANN staff report. In this report, the drafting committee
suggested three areas in which the registrars’ Model Dispute Resolution
Policy should be revised. First, in determining whether a domain name
has been registered in bad faith, consideration should be given to
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; 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 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. Second, there should be
a general parity between the appeal rights of complainants and domain
name holders. Third, the dispute policy should seek to define and
minimize reverse domain name hijacking. The draft implementation
documents attempted to respond to these concerns.

The following month, after a period for public comment, ICANN
adopted a second set of implementation documents, which had not been
meaningfully changed from the first. The two sets of implementation

mandatory administrative proceeding in the event that a third party
(a “complainant”) asserts to the applicable Provider, in compliance
with that Provider's rules of procedure, that (i) your domain name is
identical or misleadingly similar to a trademark or service mark in
which the complainant has rights; and (ii) you have no rights or
legitimate interests in respect of the domain name; and (iii) your
domain name has been registered and is being used in bad faith.

Evidence of Registration and Use in Bad Faith. For the
purposes of Paragraph 4(a)(iii), the following, in particular but
without limitation, shall be evidence of the registration and use of
a domain name in bad faith: (i) offer to sell, rent or otherwise
transfer the domain name registration to the complainant who is the
owner of the trademark or service mark or to a competitor of that
complainant, for valuable consideration; or (ii) your attempt to
attract, for financial gain, Internet users to your website or other on-
line location, by creating confusion with the trademark or service
mark of the complainant; or (iii) your registration of a domain name
in order to prevent the owner of the trademark or service mark from
reflecting the mark in a corresponding domain name, provided that
a pattern of such conduct has been established on your part; or (iv)
your registration of a domain name in order to disrupt the business
of a competitor.

Id. ¶¶ 4(a)-(b)

63. See First ICANN Staff Report, supra note 61.
64. See id.
65. See infra note 67.
66. See Second Staff Report on Implementation Documents for the Uniform Dispute

Pagination incorrect - Not for Citation
documents responded to the major criticisms of the registrars’ Model Dispute Resolution Policy. The resulting Uniform Domain Name Dispute Resolution Policy (“Uniform Policy”) became fully effective on January 3, 2000.

The Uniform Policy and its accompanying rules are incorporated by reference into all registration agreements with approved registrars and purport to “set[] forth the terms and conditions in connection with a dispute between [the registrant] and any party other than [the registrar] over the registration and use of an Internet domain name registered by [the registrant].” The Policy requires all domain name registrants to submit to a mandatory administrative proceeding upon the complaint by a trademark owner. In the event the mark owner prevails in this proceeding, the Policy provides for the transfer of the domain name to the complainant.

To prevail on a claim under the Uniform Policy, a trademark owner must prove: (i) the registrant’s domain name is “identical or confusingly similar to a trademark or service mark in which the complainant has rights”; (ii) the registrant has “no rights or legitimate interests in respect of the domain name”; and (iii) the domain name “has been registered and is being used in bad faith.”

The registrant may show that she has “rights or legitimate interests” with respect to the domain name by demonstrating:

(i) before any notice to [her] of the dispute, [her] use of, or demonstrable preparations to use, the domain name or a name

---

69. See Timeline for the Formation and Implementation of the Uniform Domain-Name Dispute-Resolution Policy, at http://www.icann.org/udrp/udrp-schedule.htm (last visited Nov. 8, 2001).
71. Uniform Policy, supra note 68, ¶ 1.
72. See id. ¶ 4.
73. See id. ¶ 4(i).
74. Id. ¶ 4(a).
corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) [she] (as an individual, business, or other organization) [has] been commonly known by the domain name, even if [she has] acquired no trademark or service mark rights”; or

(iii) [she is] 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.75

This list is meant to be non-exhaustive.76

With respect to the third element, the complainant may prove bad faith by showing any of the following four circumstances:

(i) circumstances indicating that you [i.e., the registrant] have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

75. Id. ¶4(c).
76. See id. (“Any of the following circumstances, in particular but without limitation,” if proven, will demonstrate registrant’s right to and legitimate interest in the domain name.)

PAGINATION INCORRECT - NOT FOR CITATION
(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location. 77

As above, this list is meant to be non-exhaustive. 78

2. Proper Scope of the Uniform Policy

The Uniform Policy was not meant to grant relief to every domain name registration that violates trademark law. Rather, the Uniform Policy was meant to be confined to abusive cases of cybersquatting and cyberpiracy where the registrant has no legitimate claim to the domain name. The White Paper stipulated:

[I]t should be clear that whatever dispute resolution mechanism is put in place by the new corporation, that mechanism should be directed toward disputes about cybersquatting and cyberpiracy and not to settling the disputes between two parties with legitimate competing interests in a particular mark. Where legitimate competing rights are concerned, disputes are rightly settled in an appropriate court. 79

77. Id. ¶ 4(b).
78. See id. (“The following circumstances, in particular but without limitation,” if proven, will demonstrate “registration and use of a domain name in bad faith.”).
79. White Paper, supra note 50, at 31, 747; see also The Thread.com, LLC v. Poploff, WIPO Case No. D2000-1470 (Jan. 5, 2001), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-1470.html (last visited Nov. 8, 2001) (“This Panel is not a general domain name court, and the Policy is not designed to adjudicate all disputes of any kind that relate in any way to domain names. Rather, the Policy is narrowly crafted to apply to a particular type of abusive cybersquatting.”)

pagination incorrect - not for citation
The virtues of maintaining two avenues for relief — arbitration under the Uniform Policy and litigation in a court — were recognized in the very first panel decision. A cybersquatter had registered a domain name identical to a trademark owned by the World Wrestling Federation and, three days later, sought to sell the domain name to the mark owner. In finding for the complainant, the panel noted, “Complainant acknowledged that it could have proceeded to litigation under the United States ‘Anticybersquatting Consumer Protection Act,’ but that it elected not to. By engaging in this proceeding, complainant has sought to protect complainant’s intellectual property interests while preserving the relationship between complainant and its fans at a minimal cost to all concerned.” In recognition of the limitations of arbitration, the panel in Adaptive Molecular Tech., Inc. v. Woodward, denied a domain name transfer on the grounds that the existence of disputed legal issues made the case “inappropriate for resolution under the Policy.” There had been a contention by the respondent that it was the complainant’s distributor and that the registration of the domain name was a fair use of the trademark.

IV. ANALYSIS OF THE UNIFORM POLICY AND ITS APPLICATION

The Uniform Domain Name Dispute Resolution Policy is an improvement over the NSI Dispute Policy. By offering a resolution to the abusive cases and allowing court proceedings when applicable, the Policy provides a cheap and quick method of disposing of most cases of cybersquatting.

However, the Uniform Policy seeks to accomplish too much. Procedurally, it resolves disputes more properly left to the courts. Domain name registrants with arguably legitimate claims are being
forced to transfer their registrations to trademark owners without a proper trial, and then must race to court if they wish to retrieve the domain names. More dangerously, however, the Uniform Policy in its words and application substantively extends the reach of trademark law by taking properly held domain names from registrants and giving them to the mark owners without any legal basis.

This Section will examine how the Uniform Policy, as well as the administrative panels that interpret and implement it, exceed their legal authority under U.S. law. First, it will deal generally with the problem of reverse domain name hijacking, wherein a mark owner, typically a large firm, brings an action under the Uniform Policy in order to obtain a monopoly on all domain names similar to its trademarks, regardless of the legitimacy of the current mark owner’s use. Second, it will examine the tarnishment doctrine as used by the Uniform Policy. Despite the apparent terms of the Policy and the decisions by the administrative panels, the act of tarnishing a trademark should not give rise to liability under the Policy. Punishment for trademark tarnishment is a form of speech suppression, and courts — not arbitration panels — should be performing the necessary balancing between the rights of a trademark owner and the free speech interests of the critic. Finally, this Section examines a category of recent cases where both of these problems are highlighted.

85. Although this Note focuses on the relationship between U.S. law and the Uniform Policy, it should be noted that the Policy was intended to be global in scope and does not specify any controlling national law. See Rules, supra note 70, ¶ 15(a) (“A Panel shall decide a complaint on the basis of ... these Rules and any rules and principles of law that it deems applicable.”). Panels have often applied the law of the country where the parties are domiciled. See Berkman Center for Internet & Society, Analysis of Key UDRP Issues, at http://eon.law.harvard.edu/udrp/analysis.html#choice (last visited Nov. 8, 2001) (discussing choice of law considerations in panel decisions); see also Loblaws, Inc. v. Yogeninternational, DeC Case No. AF-0164 (June 9, 2000)(applying Canadian law of statutory construction to determine the intent of the Uniform Policy’s framers), at http://www.eresolution.ca/services/dnd/decisions/0164.htm (last visited Nov. 8, 2001); Ass’n of British Travel Agents Ltd. v. Sterling Hotel Group Ltd., WIPO Case No. D2000-0086 (Mar. 29, 2000) (applying English law to determine when a site is being “used” in bad faith), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0086.html (last visited Nov. 8, 2001). However, at least one panelist has noted a tendency to apply the law of the panelist’s home country, regardless of the residency of any party. See Tourism and Corporate Automation Ltd. v. TSI Ltd., DeC Case No. AF-0096 (Mar. 16, 2000), at http://www.eresolution.ca/services/dnd/decisions/0096.htm (last visited Nov. 8, 2001), cited in Berkman Center for Internet & Society, supra.
A. Reverse Domain Name Hijacking

A flaw of the NSI Dispute Policy was its facilitation of reverse domain name hijacking, since a trademark owner could easily put a hold on a registrant’s domain name without any showing of trademark infringement. Even if the alleged infringer had a right to use the domain name, the prospect of going to trial (where fines may be levied) was enough to persuade many domain name holders to settle with the complainant.

This danger was recognized by ICANN, and the Rules for the Uniform Policy explicitly forbid reverse domain name hijacking, defined as “using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.” The substantive prevention of reverse domain name hijacking is located in paragraph 4(c) of the Uniform Policy, which provides that the domain name holder may escape liability by demonstrating his right to and legitimate interest in the domain name.

The Uniform Policy remains deficient in at least two respects. First, as Professor Froomkin argues, there remains virtually no punishment for reverse domain name hijackers. The only penalty provided by the Rules (other than denying the transfer) is that the decision reporting a bad faith complaint must be published. Although this punishment may be inadequate, it is difficult to envision a more harsh sanction without giving arbitrators more power than simply that of transferring or canceling domain names.

The more dangerous problem with the Uniform Policy is that its substantive portions do not serve to effectively block reverse domain name hijackers. In fact, the Policy could be used as a means to facilitate
this activity. Under the NSI Policy, a reverse domain name hijacker would be forced to bear the expense of going to court, a prospect that would presumably filter out some bad faith claims. However, under the cheap and easy Uniform Policy, a trademark owner can grab any domain names that are similar to its trademark while bearing only the expense of the panel,92 which could range from $950 to $2,000 for a single-member panel, exclusive of attorney’s fees.93

Even if the provisions of the Uniform Policy were written to prevent reverse domain name hijacking more explicitly, it remains up to the panel to properly enforce these terms. However, since the beginning of the dispute resolution process, some panels have shown frighteningly little regard to the requirements of the dispute resolution policy, both in terms of the “no rights or legitimate interests” requirement and the “bad faith” requirement. In several cases, instances of arguable domain name hijacking have been ignored and the domain name transferred without much argument.

In Fiber-Shield Industries, Inc. v. Fiber Shield LTD,94 the complainant, the registered trademark owner of “FIBER-SHIELD,” brought a complaint against a Canadian corporation, seeking the transfer of the domain name “fibershield.net.” Under the Uniform Policy, the respondent had a legitimate interest in the domain name since there was evidence that it had been commonly known by the domain name.95 In addition, there did not seem to be any evidence of bad faith on the part of the respondent.96 However, the panel transferred the domain name to

---

92. See Uniform Policy, supra note 68, ¶ 4(g) (“All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this policy shall be paid by the complainant . . . .”). The respondent pays half the fee if he or she requests a three-member as opposed to a one-member panel. See id. In exceptional cases, the respondent may have to pay some of the fees. See Rules, supra note 70, ¶ 19(d).


94. NAF Case No. FA92054 (Feb. 29, 2000), at http://www.arbforum.com/domains/decisions/92054.htm (last visited Nov. 8, 2001) [hereinafter Fiber-Shield].

95. See id. (“Respondent has been incorporated and has been doing business in Canada under the name ‘Fiber Shield (Toronto) LTD.’”)

96. See id. (finding that the respondent tried to register “fiber-shield.com,” claiming it did not know of the complainant’s business activity, and, discovering that the complainant already owned that domain name, registered “fibershield.net”). There was no evidence of an offer to sell the domain name or of any intent to divert customers.
the complainant because the “respondent does not claim any rights superior to the trademark registration of complainant of the name ‘fibershield.’ . . . ” 97 While this may be true, the fact alone does not require the transfer of the domain name. The Uniform Policy explicitly stipulates that the registrant can show a legitimate interest in a domain name “even if [the holder has] acquired no trademark or service mark rights.” 98 Thus, a trademark owner, merely by owning a mark, is not automatically entitled to domain names encompassing all permutations of the mark; some malfeasance on the part of the domain name holder is required. Therefore, even though the Fiber-Shield panel found that the respondent registered “fibershield.net” with “actual awareness” of a confusingly similar prior registration (the complainant had already registered “fibershield.com”), 99 this finding alone is not enough for a transfer of the domain name. Under the Uniform Policy, if a domain name holder is legitimately using a domain name, the complainant is not entitled to the domain name, regardless of whether or not the holder knew of the complainant’s confusingly similar registration.

The tolerance of reverse domain name hijacking occurs in other panel decisions as well. In Home Interiors & Gifts, Inc. v. Home Interiors, 100 the complainant owned registered trademarks in “Home Interiors” and “Home Interiors & Gifts.” It filed a complaint against the registrant of “homeinteriors.net” and “homeinteriorsandgifts.com.” The panel did not find that any of the activities constituting bad faith were met, but transferred the domain name nonetheless. The panel justified its decision by analyzing the likelihood of customer confusion, but did not offer any reason for finding bad faith. 101 Although victims of reverse domain name hijacking could feasibly seek court review of the panel’s ruling, this possibility may be somewhat illusory. 102 The losing respondent is at a significant disadvantage in the court review process. 103 The difficulty of obtaining review of a panel
decision is due primarily to the fact that the losing registrant has only ten
days to file a complaint in court before the domain name is transferred.104
This is especially constraining for registrants who have not yet retained
an attorney, or for foreign domain name registrants who must either file
a complaint in the U.S. (and thus lose their home forum) or file under the
procedures of their home country (which may not be amenable to a ten-
day filing requirement).105 On the other hand, a losing complainant can
wait indefinitely before seeking court review.

B. Tarnishment and Free Speech

In addition to facilitating reverse domain name hijacking, the
Uniform Policy also endangers free speech by punishing trademark
tarnishment. Tarnishment of a trademark is essentially prohibited in
Section 4(c), which states that a respondent who is neither running a
commercial site nor is “commonly known” by the domain name can only
show a right or legitimate interest in the domain name if he or she is
“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.”106 As a result, the
Uniform Policy’s “fair use” exception is not available when the
registrant is “tarnishing” the trademark incorporated in a domain name.

This Section argues that such a restriction on the content of a
registrant’s website runs counter to constitutional conceptions of free
speech. Even if ICANN meant the definition of “tarnishment” to be no
wider than the term as it is used in dilution law, some panels have been
extending the definition in order to cover legitimate criticism sites. In
these cases, courts should be balancing the rights of trademark owners
against the free speech interests of registrants. The following Section
first explores the appropriateness of subjecting the Uniform Policy to
constitutional standards when U.S. parties are involved and argues for
the need for greater court involvement when a dispute involves issues
other than simple cybersquatting and cyberpiracy. It then examines how
panels have suppressed free speech and criticism by exploiting the
tarnishment clause of the Uniform Policy,
1. Applicability of the Constitution to the Uniform Policy

Although it is tempting to subject ICANN to constitutional standards prohibiting the regulation of speech, the continuing vitality of the state action doctrine presents a major obstacle. Simply put, the state action doctrine recognizes that most provisions of the Constitution and the Bill of Rights apply only to governmental actors. As the Supreme Court said in an early civil rights case, “[i]t is state action of a particular character that is prohibited [by the Fourteenth Amendment]. Individual invasion of individual rights is not the subject-matter of the amendment.” Despite extensive criticism and the difficulty of making a public/private distinction in every case, courts have continually upheld the state action doctrine.

The state action doctrine has been applied explicitly to cyberspace. In Cyber Promotions, Inc. v. America Online, the Eastern District of Pennsylvania allowed America Online (“AOL”) to prevent Cyber Promotions from sending unsolicited mail to AOL subscribers. Relying on the state action doctrine, the court held that, although AOL provided free e-mail services to the public, it was not performing “an essential public service” and therefore did not assume the status of a public actor.

Because of the continuing acceptance of the state action doctrine by the judiciary, it is difficult to sustain an argument that the First Amendment should automatically apply to the Internet without further analysis, as some commentators have argued. For example, in a recent book, Lawrence Lessig contended that free speech considerations are

107. For example, the First Amendment provides, “Congress shall make no law . . . abridging the freedom of speech . . . .” and the Fourteenth Amendment reads, “No State shall make or enforce any law which . . . .” U.S. CONST. amends. I, XIV (emphasis added).
112. Cyber Promotions, 948 F. Supp. at 442; see also Berman, supra note 110, at 1283–84.
vital to the functioning of the Internet, even if these considerations mean preventing private parties from regulating speech.\footnote{113} According to Lessig, even though some view “regulation by private actors as beyond the scope of constitutional review[,]” we “should not get caught up in the lines that lawyers draw . . . .”\footnote{114} Ultimately, however, such a view is incompatible with current judicial thought.

Despite the state action requirement, ICANN should still be subject to basic First Amendment ideals in cases involving U.S. subjects. Unlike America Online, ICANN has been viewed as “quasi-public.”\footnote{115} As one commentator noted, “The private ordering that has come to dominate the Internet is premised on the underlying support of the state and other quasipublic institutions, such as ICANN.”\footnote{116} The Supreme Court has extended the reach of the First Amendment to cover certain private activities that resemble state actions. For example, in Amalgamated Food Employees Union v. Logan Valley Plaza,\footnote{117} the Court recognized that a privately-owned shopping mall was sufficiently similar to the public forum of a business district and therefore could not restrict the free speech rights of protestors.\footnote{118} Although the Court subsequently backed off this broadly inclusive definition of “state actor,”\footnote{119} it is evident that the Internet — like suburban shopping malls — can be considered “the functional equivalent of a ‘business block’ and for First Amendment purposes must be treated in substantially the same manner.”\footnote{120} “The more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it.”\footnote{121} The argument in favor of applying the First Amendment to ICANN’s activities is strengthened by the fact that ICANN obtained its authority over the Internet directly from the United States government.\footnote{122} Some commentators have argued that,
Harvard Journal of Law & Technology

Since the Internet seems like public space and the quasi-public ICANN behaves like and derives its power from the government, the public/private distinction should not apply to the Internet.123

Other scholars recognize that the state action doctrine is still very much a part of the American legal system and is probably not applicable to public-seeming private actors, but nonetheless argue that the norms and ideals behind the Constitution should be applied to the Internet. Paul Schiff Berman labels this line of argument “constitutive constitutionalism.”124 According to Berman, constitutive constitutionalism is “the idea that the Constitution might appropriately be viewed as a touchstone for articulating constitutive values and for structuring public debate about fundamental social and political issues.”125 Berman gives three reasons why we as a society should apply constitutional values to disputes, even when “ordinary law”126 should be the proper frame of analysis:

First, the symbolic power of the Constitution permits courts adjudicating constitutional claims to play a rhetorical role in articulating national values. Second, courts applying constitutional norms may sometimes be a

123. See, e.g., Margaret Jane Radin & R. Polk Wagner, The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace, 73 CHI.-KENT L. REV. 1295 (1998). According to Radin and Wagner, “all law is ‘public’ [since] the ‘private’ legal regimes of property and contract presuppose a ‘public’ regime of enforcement and policing, a baseline of background rights.” Id. at 1295. This is especially true since “a private body, NSI [now ICANN], located in the U.S. and operating under U.S. auspices, has been able to dole out ‘virtual land’ in Cyberspace (in the form of domain name space).” Id. at 1308. For this reason, Radin and Wagner argue, the public/private distinction should not apply to the Internet, and NSI should be subject to constitutional restraints.

124. Berman, supra note 110, at 1290.

125. Id. Berman distinguishes his analysis from Radin and Wagner’s, which he labels the “incoherence critique” of the state action doctrine. Id. at 1278. The incoherence critique argues that “the state action doctrine is incoherent because the state always plays a major role, implicitly or explicitly, in any legal relationship.” Id. at 1279. On the other hand, the constitutive constitutionalism theory recognizes that “there is no indication that courts will be any more likely to erode the public/private distinction in cyberspace than they have been in ‘real’ space.” Id. at 1283 (citing Cyber Promotions, Inc. v. America Online, 948 F. Supp. 436 (E.D. Pa. 1996)). Consequently, Berman suggests focusing “on the Constitution’s constitutive role in our cultural life, regardless of whether that life is lived in the public or private sphere.” Id. at 1289.

126. Berman distinguishes between “constitutional law,” which has traditionally applied only to state actions, and “ordinary law,” which applies to all other disputes. See id. at 1287–88 (citing Kay, supra note 109, at 338–39). Berman argues that Kay’s distinction is subject to challenge both on normative and descriptive grounds, since it does not recognize the cultural value of constitutional adjudication or “accord with most people’s intuitive understanding of the nature of constitutional rights.” Id. at 1288.
superior forum for addressing divisive political issues. And third, constitutionalizing a debate may encourage a more fruitful discourse in the society at large, because the relatively abstract values enshrined in the Constitution encourage participants to stake out moral philosophical claims.127

In the context of the Uniform Policy, Berman’s argument has particular significance. People use the Internet as more than merely a commercial medium. As is true with large shopping centers, the Internet is a forum that the public utilizes to express itself, and a domain name gives a speaker a name with which to attract listeners. While the right to choose such a name could conflict with other considerations such as trademark rights, it is essential that we employ the norms generated by two centuries of constitutional experience in order to resolve such disputes. As Berman argues,

[A] broader view of the Constitution’s scope would reach the private standard — setting bodies — which now function so powerfully (yet so invisibly) to establish the code that regulates cyberspace — and subject them to constitutional norms of fair process and judicial review. This approach might also provide a constitutional forum for debating many of the criticisms leveled at ICANN on account of its claimed lack of public participation and transparent processes.128

Once we accept that the Constitution has a major role to play in resolving domain name disputes that involve legitimate criticism sites, it appears as though ICANN dispute resolution panels are inappropriate vehicles for generating uniform decisions regarding fundamental policy choices. In his book Imperfect Alternatives, Neil K. Komesar compares various institutions available to us for performing legal processes.129 On one hand, Komesar recognizes that many cases can and should be adjudicated outside the judicial setting. The “rules, procedures, and practices raise the costs of participation in the adjudicative process [i.e., the courts] so high that many important issues, although handled badly

127. Id. at 1290.
128. Id. at 1307.

Pagination incorrect - not for citation
Therefore, issues such as cybersquatting could be handled by arbitration panels, which can decide basic questions of trademark ownership and infringement at a low cost.

On the other hand, when issues of free speech arise in a domain name dispute, the court system is the only viable institution that can resolve these questions. As Komesar notes, “Th[e] expensive independence [of the judiciary] provides important comparative advantages for the adjudicative process. Severe biases in the other institutions, in particular the political process, are sometimes avoided or reduced in the adjudicative process.” As explained above, there has been evidence of pro-big business bias in the first set of panel decisions.

In addition to the importance of avoiding bias, we should insist on judges deciding constitutional issues because “[m]ore than the officials in any other institutions, judges have the freedom and the responsibility to decide based on broad social considerations.” In particular, “speech cases require the judiciary to make difficult substantive decisions.” Berman has noted that:

[U]nhlike legislatures, which “see their primary function in terms of registering the actual, occurrent preferences of the people,” courts may be more “ideologically committed [and] institutionally suited to search for the meaning of constitutional values.” Because of this difference... judges may be uniquely qualified to be the final arbiters on issues involving fundamental social values.

The importance of having a coherent and just policy to deal with speech interests on the Internet outweighs the need for quick and cheap answers to trademark questions. As Berman notes, “articulating foundational principles can be as important as providing a fixed resolution to possible future cases.” The Internet is the newest medium for communication, and we should not contract out the major

130. Id. at 149.
131. Id. at 150.
132. See supra Section III.A.
133. KOMESAR, supra note 129, at 150.
134. Id. at 208.
136. Berman, supra note 110, at 1308.
policy decisions to a private not-for-profit agency. For free speech rights on the Internet to be consistently and deliberately applied, it must be the judiciary that makes the substantive decisions.

2. The Suppression of Legitimate Criticism by Dispute Resolution Panels

As discussed above, the Uniform Policy allows for the transfer of a domain name where the registrant uses it to “tarnish” a trademark. This language has been used by panels to transfer domain names from a registrant, who is often operating a criticism site, to the trademark owner being criticized. These types of decisions — balancing the free speech rights of the registrant against the trademark rights of the complainant — should be resolved by a court.

On a basic level, the invocation of a tarnishment rationale is misplaced in a dispute resolution policy designed to “be directed toward disputes about cybersquatting and cyberpiracy and not to settling the disputes between two parties with legitimate competing interests in a particular mark.” Apart from the tarnishment language, the remainder of the Uniform Policy, which focuses on clearer cases of cyberpiracy and cybersquatting, is appropriate for resolution by an arbitration panel, as argued above.

However, preventing registrants from showing a legitimate interest in a domain name merely because they tarnished the associated trademark dangerously encroaches upon their freedom of speech, particularly when panels equate “tarnishment” with “criticism.”

---

137. As Lessig has argued, “If code functions as law, then we are creating the most significant new jurisdiction since the Louisiana Purchase, yet we are building it just outside the Constitution’s review. Indeed, we are building it just so that the Constitution will not govern — as if we want to be free of the constraints of value embedded by that tradition.” LESSIG, supra note 113, at 217.

138. White Paper, supra note 50, at 31,747; see also Second ICANN Staff Report, supra note 66, ¶ 4(1)(c) (“Except in cases involving ‘abusive registrations’ made with bad-faith intent to profit commercially from others’ trademarks (e.g., cybersquatting and cyberpiracy), the adopted policy leaves the resolution of disputes to the courts . . . .”).

139. See, e.g., Mission KwaSizabantu v. Rost, WIPO Case No. D2000-0279 (June 7, 2000), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0279.html (last visited Nov. 8, 2001) (“The admitted nature of the use of the domain names in a website includes alternative views and indeed critical views concerning the Complainant and its activities. The Panel holds such activity amounts to tarnishing the activities associated with the trademark or service mark ‘KwaSizabantu’, and this is sufficient to fail point (d) of the test.” To be fair, however, several panels have rejected this view. See, e.g., Bridgestone Firestone, Inc. v. Myers, WIPO Case No. D2000-0190 (July 6, 2000), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0190.html (last visited Nov. 8, 2001); Britannia Bldg. Soc’y v. Britannia Fraud Prevention, WIPO Case No. D2001-0505 (July 6, 2001), at http://arbiter.wipo.int/domains/decisions/ html/2001/d2001-
commentators argue that there is a substantial risk that the Policy’s language can be used to deny protection to legitimate criticism sites.\footnote{140} In addition, panels in other countries may construe “tarnishment” much more broadly than it has been interpreted by U.S. courts in dilution cases.\footnote{141}

Based on the mere language of the Uniform Policy, the danger envisioned by these commentators seems exaggerated. First, the tarnishment language only negates one method of demonstrating legitimate use.\footnote{142} Second, the trademark owner still must show bad faith in both the registration and use of the domain name. Third, ICANN has recognized the danger of reading the tarnishment language more broadly than dilution law would suggest and in its Staff Report has limited “tarnishment” to include only “acts done with intent to commercially gain.”\footnote{143}

However, some panels have ignored the limitations imposed by the language of the Policy and have transferred domain names simply because the registrants had tarnished existing trademarks. In a growing line of cases, panels have issued decisions against registrants who had used a domain name that combined a trademark with a disparaging word (for example, “guinness-beer-really-really-sucks.com”\footnote{144}). This category of cases will be examined below, since the decisions frequently involve both reverse domain name hijacking and free speech issues.\footnote{145}

In another group of cases, panels were imprecise in distinguishing between the trademark holder’s requirements to show non-legitimate use of a domain name and to show bad faith in registration and use of a domain name. Frequently, the panels blurred these two elements, both

\footnote{140}{See Froomkin, supra note 88, at Substantive Issues: Critical Issues: Tarnishment; infra § III.C.}
\footnote{141}{See Froomkin, supra note 88, at Substantive Issues: Critical Issues: Tarnishment.}
\footnote{142}{However, it is the only method for the registrant who has not used the domain name either in connection with herself or with the offering of goods or services.}
\footnote{143}{See Second ICANN Staff Report, supra note 66, n.2, which states: Several commentators indicated that the concept of “tarnishment” in paragraph 4(c)(iii) might be misunderstood by those not familiar with United States law or might otherwise be applied inappropriately to noncommercial uses of parody names and the like. Staff is not convinced this is the case, but in any event wishes to point out that “tarnishment” in paragraph 4(c)(iii) is limited to acts done with intent to commercially gain. Staff intends to take steps to publicize this point.}
\footnote{145}{See infra § III.C.}
of which the trademark owner must prove to prevail. For example, in *Ingersoll-Rand Co. v. Gully*, the registrant used the “ingersoll-rand.net,” “ingersoll-rand.org,” and “ingersollrand.org” domain names to link to two pornographic sites. The panel admitted that none of the circumstances listed in paragraph 4(b) of the Uniform Policy (which specify circumstances amounting to bad faith registration and use) was applicable to the case. However, the panel stated that “the tarnishment rationale set out in the case of *Panavision International v. Toeppen* is applicable to the present situation, where the domain names were used by Respondent [the registrant] as links to pornographic sites,” and, for this reason, there was bad faith registration and use of the domain name. While the registrant’s use of the domain name may violate dilution law and the ACPA, it should be beyond the scope of the dispute resolution process to transfer domain names based purely on a tarnishment theory. For example, the panel found that “there is no evidence or suggestion that Respondent’s use of the links to pornographic sites was intended either as satire or as protected comment.” This determination, reaching constitutional proportions, is one properly left to the courts.

The excessive reliance upon tarnishment as disqualifying a registrant from holding a domain name that incorporates a trademark stems partly

---


147. *See id.* The panel correctly decided that using the domain to offer links to pornographic sites does not fulfill the 4(b)(iii) requirement of intentionally attracting for commercial gain users to the site by creating a likelihood of confusion with the owner’s trademark as to the source, sponsorship, affiliation, or endorsement of the site, since it is “highly unlikely that such Internet users, who were seeking the web site of a long-standing United States corporation, were likely to be confused that the Complainant would deign to sponsor such links as <tasteless.net> or <rascals.net>, or endorse the products or services offered there.” *Id.*

148. *Id.* (referring to Panavision Int’l v Toeppen, 945 F. Supp. 1296, 1304). The other evidence of bad faith the panel finds is similarly unconvincing. The panel finds bad faith because, “Respondent has failed to respond to the offer by the trademark holder to purchase the domain names at Respondent’s out of pocket costs.” *Id.* The mere refusal to turn over a domain name that does not, according to the Uniform Policy, infringe upon the rights of the trademark owner cannot itself amount to bad faith. Otherwise, the required showing of bad faith would be superfluous. *Cf. Home Interiors & Gifts, Inc. v. Home Interiors, WIPO Case No. D2000-0010* (Mar. 7, 2000) (finding non-legitimate interest in domain name because of refusal to sell to trademark owner), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0010.html (last visited Nov. 8, 2001).

149. Ironically, the panel does not determine whether the complainant’s mark is famous (as would be required by dilution law, under which *Panavision* was decided), stating that such a determination is “currently outside the scope of the mandate of this Panel.” Ingersoll-Rand, WIPO Case No. D2000-0021.

150. *Id.*
from ICANN’s lack of guidance. While a Staff Report announced an intention to limit “tarnishment” to “acts done with intent to commercially gain,” ICANN has thus far taken no steps to publicize this interpretation.

V. &TradeMark; sucks.com: A Case Study

In recent months, several large corporations have taken the offensive against potential critics by registering dozens of domain names that incorporate their trademark in a disparaging manner. As of September 2000, nearly 250 companies registered defamatory versions of their domain names. With over 200 registered sites, Wal-Mart Stores topped the list. While critics claim that these large corporations’ actions are aimed at stifling legitimate criticism, the trademark owners claim that they are only protecting their trademarks, stating, for example, “It is unacceptable for people to use our name in vain.”

Companies like Wal-Mart have not stopped at registering unowned domain names. As of the end of 2000, Wal-Mart had filed nine complaints under the Uniform Policy contesting fifteen domain names. Of these, six domain names related to a disparaging use of the Wal-Mart name. In these cases, as well as in a large proportion of similar cases involving other complainants, the respondents had registered the name of a well-known business with the addition of the word “sucks.”

151. Second ICANN Staff Report, supra note 66, n.2; see also supra note 143.
152. See David Streitfeld, Making Bad Names for Themselves, WASH. POST, Sept. 8, 2000, at A01.
153. See id.
156. See Proceedings List, at http://www.icann.org/udrp/proceedings-list-name.htm (last visited Nov. 08, 2001).
According to a recent ACPA case, this phenomenon is “not uncommon, and is part of an Internet phenomenon known as ‘cybergripping.’” 158

The disturbing aspect of this trend is the frequency with which some panels transferred the domain name to the complainant without a careful inquiry into whether the disputed actions of the respondent fell within the activities prohibited by the Uniform Policy. The inattention to the letter and purpose of the Uniform Policy in many of these dispute resolution proceedings exemplifies the more widespread problems of reverse domain name hijacking and freedom of speech limitations.

The problem of reverse domain name hijacking in these cases stems mainly from panels that overlook portions of the Uniform Policy’s test. Since the complainants in many of the disparaging domain name cases are large companies with trademark ownership in a portion of the disputed domain name, panels tend to decide in their favor without a sufficient inquiry into whether the registrant acted incorrectly. As one commentator noted, “The reliance by the arbitration panels on the possession of a trademark or copyright sometimes leads to results that ignore other important legal considerations.” 159 By overlooking registrants’ claims that may have merit, the Uniform Policy panels assist trademark holders in overextending their rights by collecting any domain name that may incorporate their trademark.

For example, the Uniform Policy requires that the complainant prove that the domain name in question be “identical or confusingly similar to a trademark or service mark” in which the complainant has rights. 160 The underlying logic is clear — a trademark owner should not be able to extend his trademark rights beyond those domain names that a reasonable person might confuse with the mark. This requirement should not be met in many cases where, for example, the respondent registers the domain name “<trademark>sucks.com.” The domain name is not identical to the trademark, nor is it confusingly similar. At least one panel has recognized this fact. In CompUSA Mgmt. Co. v. Customized Computer Training, 161 the panel allowed the respondent to retain the domain names “stopcompusa.com” and “bancompusa.com” over CompUSA’s protests, holding “[T]here is absolutely no confusion


160. Uniform Policy, supra note 68, ¶ 4(a)(i).

or similarity, much less identity, between the domain names and the trademarks held by Complainant [CompUSA]. No one could confuse ‘COMPUSA’, or anyone [sic] of the registered trademarks, and ‘STOPCOMPUSA.COM’ and ‘BANCOMPUSA.COM’.’

The panel correctly disapproved of CompUSA’s methods:

After reading the pleadings, the Panelist is left with a bad taste. Here, a large company, faced with criticism from an individual, has attempted to use this process and procedure to stifle that criticism. If the actions and conduct of Respondent are wrongful, then Complainant has access to the courts of law, where the truthfulness of the allegations made by Respondent can be challenged. Use of this forum by Complainant in this context is inappropriate and constitutes “cyber-bullying.”

In the judicial context, courts have held the similar view that appending disparaging words to a trademark undercuts any argument of similarity for Lanham Act purposes.

---

162. Id.
163. Id.
164. See, e.g., Bally Total Fitness Holding Corp. v. Faber, 29 F. Supp. 2d 1161 (C.D. Cal. 1998). In Bally, the court found no likelihood of confusion between plaintiff’s mark and defendant’s “Bally’s sucks” website, noting that:

No reasonable consumer comparing Bally’s official web site with Faber’s site would assume Faber’s site ‘to come from the same source, or thought to be affiliated with, connected with, or sponsored by, the trademark owner.’ ‘Sucks’ has entered the vernacular as a word loaded with criticism. Faber has superimposed this word over Bally’s mark. It is impossible to see Bally’s mark without seeing the word ‘sucks.’ Therefore, the attachment cannot be considered a minor change.

Id. at 1163–64.

It should be noted, however, that the defendant’s website did not have “Bally’s” in the domain name, a fact which some panels have used to distinguish Bally’s from Uniform Policy cases. See, e.g., Wal-Mart Stores, Inc. v. Walsucks, WIPO Case No. D2000-0477 (July 20, 2000), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0477.html (last visited Nov. 8, 2001). It is unclear why this should make a difference. As Bally itself notes, ‘even if Faber did use the mark as part of a larger domain name, such as ‘ballysucks.com’, this would not necessarily be a violation as a matter of law,’ since “no reasonably prudent Internet user would believe that ‘Ballysucks.com’ is the official Bally site or is sponsored by Bally.” See Bally Total Fitness, 29 F. Supp. 2d at 1165 & n.2; see also Lucent Techs., Inc. v. Lucentsucks.com, 95 F. Supp. 2d 528 (E.D. Va. 2000).
Unfortunately, other panels ignore the likelihood of confusion requirement. Even in cases where the similarity between the trademark and domain name is expressly considered, panels tend to find a way around this problem to award the domain to the mark holder. For example, the panel in *Wal-Mart Stores, Inc. v. MacLeod* \(^{165}\) recognized that “[n]o reasonable speaker of modern English would find it likely that Wal-Mart would identify itself using wal-martsucks.com” and “specifically reject[ed] Complainant’s argument that consumers are likely to be confused as to the sponsorship or association of a domain name that combines a famous mark with a term casting opprobrium on the mark.” \(^{166}\) However, the panel transferred the domain name, arguing:

> Nevertheless, the Panel understands the phrase ‘identical or confusingly similar’ to be greater than the sum of its parts. The Policy was adopted to prevent the extortionate behavior commonly known as ‘cybersquatting,’ in which parties registered domain names in which major trademark owners had a particular interest in order to extort money from those trademark owners. This describes Respondent’s behavior. Thus, the Panel concludes that a domain name is ‘identical or confusingly similar’ to a trademark for purposes of the Policy when the domain name includes the trademark, or a confusingly similar approximation, regardless of the other terms in the domain name. \(^{167}\)

While the panel should be commended for its examination into the purposes of the Uniform Policy, its analysis went far afield from the language of the Policy. This may be a result of the fact that there was a considerable amount of bad faith on the part of the respondent, as he admitted to registering the domain name with an intent to sell it.

---


166. *Id.*

However, the panel’s reasoning may be used in the future to grant trademark owners over-inclusive rights over a range of criticism sites.168 As commentators have observed, “What is most instructive in these cases is less the outcome . . . and more the reasoning of the panelists, reasoning on which future panel decisions will increasingly rely.”169

Even more disturbing than the over-extension of trademark rights given to mark owners is the concurrent loss of fora for criticism. Two commentators conducted a study of six panel decisions dealing with criticism through the incorporation of a trademark in the registrant’s domain name in the months of August and September 2000.170 In those decisions, every panel paid homage to the value of criticism; however, the panels transferred four out of six domain names.171

In one case, Wal-Mart sought to acquire a series of disparaging domain names from Kenneth Harvey, a Canadian author.172 Harvey claimed that his websites, under such domain names as “walmartcanadasucks.com” and “walmartpuertoricosucks.com,” were “currently up and running as freedom of expression forums of complaint against Wal-Mart.”173 He also claimed that he never sought to sell the domain names to Wal-Mart, and that his animosity toward Wal-Mart stemmed from a previous panel decision where Wal-Mart obtained the domain name “walmartcanada.com.”174 Interestingly, Wal-Mart responded to the free speech issues, claiming that ICANN was not a government agency and therefore was not limited by the First Amendment.175 However, the panel transferred the domain names

---


170. See id. (analyzing six cases “highlighting the clash between the right of free expression on the Internet and the intellectual property rights of the mark holder”).

171. See id.; see also Halpern & Mehrotra, supra note 51, at 560 (“ICANN’s Policy currently does little to protect individuals who use websites to parody or criticize trademark holders.”).


175. See Walsucks, WIPO Case No. D2000-0477. Wal-Mart claimed: [U]nder both U.S. and Canadian law, speech is not entitled to absolute protection under all circumstances. Speech is only
protected against governmental interference. Where the speech does not involve an activity or institution controlled by the government, there may not be any special protection . . . ICANN is . . . a non-profit, private corporation, not a governmental entity. This domain name dispute procedure is not a governmental process or activity, and WIPO is not a governmental institution; therefore, the Complaint does not represent governmental interference with claimed protected speech.

This Wal-Mart case should be contrasted with another case, decided only four months later. In Wal-Mart Stores, Inc. v. wallmartcanadasucks.com, Wal-Mart once again attempted to obtain the transfer of a defamatory domain name, “wallmartcanadasucks.com,” from Kenneth Harvey. In this case, the sole panelist found for Harvey, writing, “[I] do not see how a domain name including ‘sucks’ ever can be confusingly similar to a trademark to which ‘sucks’ is appended,” and found that, “[t]he use of the SUCKS.COM suffix attached to a company name has become a standard formula for internet sites protesting the business practices of a company.” Despite the previous panel decision that held that “wallmartcanadasucks.com” was confusingly similar to the complainant’s trademark, the panelist in the more recent case

protected against governmental interference. Where the speech does not involve an activity or institution controlled by the government, there may not be any special protection . . . ICANN is . . . a non-profit, private corporation, not a governmental entity. This domain name dispute procedure is not a governmental process or activity, and WIPO is not a governmental institution; therefore, the Complaint does not represent governmental interference with claimed protected speech.

Id.

176. Id.
177. First, it was not clear that this claim for a fee was either in exchange for a domain name or with an intent to divert Wal-Mart customers, as required by the Uniform Policy. Second, the registrant claimed his request for a fee was a joke, playing on the fact that “[Wal-Mart has] spent thousands and thousands of dollars on these things, Wal-Mart with hyphens, WalMart without, which is ridiculous. These guys are going out sucking up everything they possibly can to try to prevent people from complaining about them on the Internet.” See Pigg, supra note 172, at BU01. Finally, there is the question whether a reasonable customer would mistake a website posted at the domain name “wallmartcanadasucks.com” for an authentic Wal-Mart site.

178. See Johnson, supra note 159, at 428.
180. The only difference between this domain name and the one involved in the earlier proceeding is an extra “L” in the word Wal-Mart. This deliberate misspelling does not seem to have played any part in the panel’s decision. See id.
181. Id. The panelist based his decision in large part on the decisions of Bally Total Fitness Holding Corp. and Lucent Technologies, Inc. See supra note 164.
182. See Wal-Mart Stores, Inc. v. Walsucks, WIPO Case No. D2000-0477 (July 20,
recognized the lack of possible confusion, as well as the importance of forums for legitimate criticism:

[D]istasteful conduct should not stampede UDRP decision makers into an unwarranted expansion of the domain name dispute process. The UDRP has a narrow scope. It is meant to protect against trademark infringement, not to provide a general remedy for all misconduct involving domain names . . . . [W]hether a use is illegal in general is beyond the subject matter jurisdiction of an administrative panel under the UDRP.

Disciplined construction of the UDRP is appropriate for another reason. The Policy should not be used to shut down robust debate and criticism. Allowing trademark owners to shut down sites that obviously are aimed at criticism of the trademark holder does just that.

The Respondent may be acting unfairly. He may be engaged in unwarranted disparagement. He may be acting childishy. He may be retaliating for having lost earlier Cybersquatting cases. But this does not necessarily mean that he may be forced to transfer the accused domain name to the complainant under the UDRP, considering the purpose.183

This decision, while laudable, does not comport with the earlier holdings of dispute resolution panels. The panelist did not make a

---

183. wallmartcanadasucks.com, WIPO Case No. D2000-1104.
184. It should be noted that the panelist delved quite deeply into trademark and copyright law, as well as the policy goals underlying the Uniform Policy.
185. In Lockheed Martin Corp. v. Parisi, WIPO Case No. D2000-1015 (Jan. 16, 2001), at http://arbiter.wipo.int/domains/decisions/html/2000/d2000-1015.html (last visited Nov. 8, 2001), the panel enumerated nine previous cases that held that a domain name incorporating a trademark plus the word “sucks” was confusingly similar to the trademark.
It listed *Wal-Mart Stores, Inc. v. wallmartcanadasucks.com* as the only decision to that date to hold the reverse.186

In the earlier case, the panel relied on the fact that Harvey requested a “consultant’s fee” from Wal-Mart, holding that this action amounted to cybersquatting. See *supra* note 177 and accompanying text. In the more recent case, the panelist rejected this reasoning, arguing, “The inference of a demand for payment for transfer of the domain name was only weakly supported in the earlier cases, and there is no basis for it in this case.” *wallmartcanadasucks.com*, WIPO Case No. D2000-1104.


190. *See Chrysta Osborn, Constitutional Scrutiny and Speech: Eroding the Bedrock Principles of the First Amendment, 44 Sw. L.J. 1013, 1015 n.33 (1990). “‘Chilling effects’ are usually discussed in conjunction with the overbreadth doctrine, but the principle that people will be intimidated from exercising their right to speak applies whenever the effects of a regulation are unknown.”* *Id.* (citations omitted) (citing
speech acts differently “diminishes the principle of equality of speech. . . . [S]uch inconsistencies tend to have a ‘chilling effect’ on speech since the inconsistencies tend to favor the regulation rather than the protected speech.”

This uncertainty should be resolved by forcing trademark owners to avail themselves of the judicial process when the registrant has a legitimate free speech claim over the domain name. The judicial system has an established means of resolving disputes among lower courts and promoting conformity. Instead of promoting the goal of conformity, the Uniform Policy frustrates it by its lack of a provision for a precedent-setting body, as well as its discouragement of court appeals from losing registrants. ICANN should amend the Uniform Policy to encourage panels to decline deciding disputes that are more complex than pure cybersquatting or cyberpiracy. Particularly in cases of arguably legitimate criticism on the part of the registrant, it is important for the court system to establish the acceptable methods of self-expression on the Internet.

VI. CONCLUSION

While in many ways the Uniform Domain Name Dispute Resolution Policy represents an improvement over litigation and the NSI Dispute Policy, it still suffers from several flaws. Trademark owners are favored in their pursuit of similar domain names at the expense of legitimate domain name registrants. In facilitating reverse domain name hijacking, the Uniform Policy allows panels to reach issues properly left to courts. These panels often favor mark owners by granting them over-extensive trademark rights. In addition, the Uniform Policy improperly allows tarnishment to play a role in determining rights in a domain name. Through the tarnishment rationale and other means, administrative panels have increasingly limited the speech interests of critics.
The Uniform Policy must be amended to provide a more equitable hearing for domain name registrants. However, more importantly, the members of the administrative panels must be more careful in applying the Policy. All too often, the panels have equated a trademark with a right to own all possible incarnations of that mark as domain names. It would be better to heed the words of Justice Oliver Wendell Holmes and remember that a trademark “is not a copyright.”194 When a trademark “is used in a way that does not deceive the public,”195 society should not prevent the public from using the trademark to tell the truth or offer an opinion in the course of speech.

195. Id.