Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy

Jacqueline D. Lipton
University of Pittsburgh School of Law, jdl103@pitt.edu

Follow this and additional works at: https://scholarship.law.pitt.edu/fac_articles

Part of the Communications Law Commons, Computer Law Commons, Intellectual Property Law Commons, and the Internet Law Commons

Recommended Citation
Available at: https://scholarship.law.pitt.edu/fac_articles/182

This Article is brought to you for free and open access by the Faculty Publications at Scholarship@PITT LAW. It has been accepted for inclusion in Articles by an authorized administrator of Scholarship@PITT LAW. For more information, please contact leers@pitt.edu, shephard@pitt.edu.
BEYOND CYBERSQUATTING:
TAKING DOMAIN NAME DISPUTES PAST
TRADEMARK POLICY

Jacqueline D. Lipton*

All good "cyberlawyers" know that, in the late 1990s, legal and regulatory measures were adopted, both at the domestic and international level, to address the then-growing problem of "cybersquatting": that is, the registration of often multiple domain names corresponding to valuable corporate trademarks with the intention of extorting high prices from the trademark owners for transferring the names to them. Since 1999, the Uniform Domain-Name Dispute-Resolution Policy ("UDRP") in particular, complemented by the Anticybersquatting Consumer Protection Act ("ACPA"), has been very successful in combating this practice. Unfortunately, since the late 1990s, there has been little movement towards developing a comprehensive system for domain name dispute resolution outside the cybersquatting area. Little thought has been given to other forms of domain name disputes that are not so well served by the UDRP and the ACPA. Examples of these kinds of disputes include certain complaints involving personal names and cultural or geographic place names, as well as disputes involving contests between two legitimate trademark holders. This Article suggests the development of a new classification scheme for different types of Internet domain name disputes outside the "bad-faith" cybersquatting context. This new classification scheme highlights both the fact that the current legal and regulatory framework is focused on only a narrow class of domain name disputes and that the policies underlying this framework are not suited to other categories of domain name disputes. The Article further identifies ways in which new solutions could be developed that are better suited to domain name complaints outside the cybersquatting context and that more appropriately reflect emerging social norms about Internet usage and domain name registration.

* Associate Professor and Associate Director, Frederick K. Cox International Law Center, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, Ohio 44106, USA, e-mail: Jacqueline.Lipton@case.edu, Fax: (216) 368-2086. The author would like to thank Professors Anupam Chander, Graeme Austin, and Cynthia Ho for valuable comments on an earlier draft of this article.
I. INTRODUCTION

What's in a name? Plenty, if it is an Internet domain name. They can be registered for fun or profit or simply to guide Internet surfers to information that might interest them. Internet domain names are big business. Unsurprisingly, it is their very capacity to serve as business assets that has skewed the way that the legal system has come to accommodate them in recent years.

In the early days of the Internet, law reviews and court reporters were filled with discussions about how the law should characterize Internet domain names, particularly in terms of their relationship with trademark law.¹ However, with the advent of the

¹ See Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117, 121-22,
Anticybersquatting Consumer Protection Act ("ACPA")\(^2\) in the United States and the Uniform Domain-Name Dispute-Resolution Policy ("UDRP")\(^3\) at a more global level, these discussions have largely died down. People simply assume that we now have a workable and efficient system in place to deal with legal disputes about who might have the superior interest in a given domain name.

The problem is that the current dispute resolution mechanisms are focused on the protection of commercial trademark interests, often to the detriment of other socially important interests that may inhere in a given domain name. If the global information society continues down the current road of protecting these interests at all costs, other important social norms relating to Internet use will not have a chance to develop, and the Internet will become permanently skewed in favor of commercial trademark interests. Thus, society will miss out on the potential to develop the Internet in general, and the domain name system in particular, in new and useful ways.

Even in the realm of purely commercial interests, the current domain name dispute resolution mechanisms are somewhat lacking. While the ACPA and the UDRP are extremely useful and effective in protecting trademark interests in the bad-faith cybersquatting context,\(^4\) they are very limited in their ability to deal with disputes

---


3. A copy of the Uniform Domain-Name Dispute-Resolution Policy may be found at http://www.icann.org/udrp/udrp-policy-24oct99.htm. (last modified Feb. 5, 2002) [hereinafter UDRP]. The UDRP was adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN") in 1999. Id.

4. For the purposes of this discussion, "cybersquatting" is conduct, usually regarded as being in bad faith, in which an individual registers one or more domain names corresponding to valuable registered trademarks with the intention of profiting by selling those names to the trademark holder(s). See Nathenson, supra note 1, at 925-26.
between two legitimate holders of similar trademarks with respect to a corresponding Internet domain name.  

The time has come to develop some new approaches to domain name disputes that can take account of interests in domain names outside the bad-faith cybersquatting context. This Article suggests a new classification scheme for different kinds of domain name disputes. The new scheme can serve as the basis for the development of new approaches to Internet domain name dispute resolution. The following discussion suggests individual remedial mechanisms that might be developed to suit each specific category of disputes. It also identifies the kinds of competing social values that will likely need to be taken into account in future development of a more comprehensive approach to domain name dispute resolution.

Part II explains the technical basis of the Internet domain name system. It describes what Internet domain names are, how they work, and why they are so commercially valuable. Part III sets out the current regulatory framework for Internet domain name disputes, focusing, as it does, on the prevention of bad-faith cybersquatting. It also considers the relationship between traditional trademark policy and these newer domain name dispute resolution procedures, suggesting that there is not necessarily a particularly comfortable or logical fit between them. Part IV develops a new classification scheme for different kinds of Internet domain name disputes. It suggests that traditional cybersquatting activities might continue to be regulated by the ACPA and the UDRP while various new classes of Internet domain name disputes might be regulated in other ways more suited to the types of legal, social, and cultural interests implicated in the dispute. Suggestions for how this may be achieved in practice are incorporated within the discussion of each new proposed category of dispute.

Part V then sets out some conclusions on these issues, noting, in particular, that time is now of the essence in developing new approaches to domain name disputes. If we do not develop these new approaches soon, we risk entrenching the current status quo. This, in turn, would likely lead to the adoption of a default regulatory policy suggesting that the only interests to be protected

---

5. This is not surprising, given that the first concern of the commercial Internet community was bad-faith cybersquatting and not other kinds of disputes, such as competitions between multiple legitimate trademarks. See World Intellectual Property Organization Arbitration and Mediation Center, New Generic Top-Level Domains: Intellectual Property Considerations, ¶¶ 12-13, at http://arbiter.wipo.int/domains/reports/newgtld-ip/printable.html (last visited Nov. 22, 2005) [hereinafter New Generic Top-Level Domains]. However, it may now be time to investigate domain name disputes with a broader focus, given the kinds of cases now arising under traditional trademark law, the ACPA, and the UDRP. See infra notes 9, 28-29, 70, 93-95, 109, 114 and accompanying text.
in the domain name context are commercially valuable trademark rights. Such an outcome would be an unfortunate occurrence that would likely contribute to the future development of the Internet as a somewhat bland commercial medium, as opposed to facilitating uses of Internet domain names that are more reflective of emerging global social values and norms outside the purely commercial context.

II. INTERNET DOMAIN NAME BASICS

An Internet domain name is an alpha-numeric mnemonic device that can be mapped onto an Internet Protocol ("IP") address to enable users to "surf the Web" more easily than if they had to remember the details of each IP address they wanted to visit. Numeric IP addresses tell a computer which World Wide Web ("Web") page to open, but are relatively meaningless to a human Internet user. Internet domain names, on the other hand, can be easily remembered because they are usually chosen in a form that relates somehow to the entity whose Web site the person might want to access: for example, microsoft.com for the Microsoft Corporation.

Clearly, a domain name can be a very valuable business asset, in that it can operate like a combination trademark and shop front that both assists customers in locating a commercial Web site and can develop goodwill in the sense of attracting customers over a period of time. Outside the purely commercial arena, Internet domain names can also be valuable in helping people find specific information, either as pointers to the information per se or as pointers to a useful source of information (such as a government information Web site, library Web site, university Web site, etc.).

Because of their uniqueness—a domain name can only map onto one IP address at a time—and because of their potential value,


7. As the ICANN Web site elaborates:

   The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address—just like a telephone number—which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name") to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a "mnemonic" device that makes addresses easier to remember.

8. Tucker, supra note 1, ¶ 90. This attribute makes domain names very different from other forms of digital information property, in that domain
the commercial and legal systems have struggled in recent years to classify the status of domain names. Are domain names a form of intellectual property or quasi property? If either, what should their precise legal attributes be? Answering these questions has proved to be somewhat more difficult in practice than one may have thought, and a detailed discussion of the proprietary attributes of Internet domain names is beyond the scope of this Article. However, it may be that the new approaches to dispute resolution advocated in this Article will alleviate the need to resolve some of these questions, at least in the context of contests between two or more parties as to who has the superior claim to a given Internet domain name.

In terms of technical infrastructure, the domain name system is administered by the Internet Corporation for Assigned Names and Numbers ("ICANN"). ICANN is a private organization that

names are unique and rivalrous, whereas other valuable digital information products, such as digital data, computer software, electronic databases, etc., all involve non-rivalrous information which can be utilized by more than one person at a time. Thus, implications for regulating domain names as a "scarce resource" under traditional property theory may be more easily made out than is the case for other forms of digital intellectual property. That discussion is outside the focus of this Article, but it is worth noting by way of comparison with other forms of digital information property.

9. See Kremen v. Cohen, 337 F.3d 1024, 1029-30 (9th Cir. 2003) (holding that domain names are a form of intangible property for the purposes of the California tort of conversion); Anupam Chander, The New, New Property, 81 TEX. L. REV. 715, 776-81 (2003) (arguing that the existence of property rights in domain names is imperative to an attempt to create a more globally equitable domain name system); Xuan-Thao N. Nguyen, Commercial Law Collides with Cyberspace: The Trouble with Perfection—Insecurity Interests in the New Corporate Asset, 59 WASH. & LEE L. REV. 37, 62-71 (2002) (discussing the importance of treating domain names as legal property in a transactional context).

10. In any event, it is arguable that the debate over property or quasi-property rights in Internet domain names has not advanced the ball very much in terms of resolving disputes over Internet domain names that do not revolve around traditional trademark interests. This Article takes what could be described as a "bottom-up" approach to the problem. That is, it identifies emerging social values and norms with respect to rights in Internet domain names and attempts to categorize disputes and possible approaches to dispute resolution in light of these social and cultural developments. Such an approach could be contrasted with a "top-down" approach, which might identify potential proprietary or quasi-proprietary attributes of Internet domain names and use those categorizations as the basis for setting out a priority scheme for resolving conflicts in domain name registration. E.g., Nathenson, supra note 1, at 925.

11. According to the organization's own Web site:

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root
manages and coordinates the domain name system by overseeing the distribution of unique IP addresses and domain names. However, actual domain name registration is handled by numerous domain name registries situated in various countries around the world.

When inserted into the address bar of an Internet browser, domain names are usually preceded by the letters “http,” which stand for “hyper text transfer protocol.” This is a set of rules that provides the means of communicating on the Web. Moreover, “http” is part of the Uniform Resource Locator (“URL”), which directs the computer to the location of the desired Web page. However, the domain name itself technically does not include the protocol through which a Web page is accessed. The domain name will generally commence with the letters “www” which indicates that the domain name is part of the Web. The important part of the domain name is what follows this prefix. It will usually include the name of the server on which the Web page is stored. This may be followed by some additional information relating to the file structure of the Web page in question.

Different files and folders on a Web site may be indicated using a backslash (“/”) in the relevant address. For example, the address http://www.icann.org/faq/#dns shows that the Web page in question is stored on the “icann” server in a folder entitled “faq” and subfolder called “#dns.” Even without being a computer programmer or Internet aficionado, one can probably guess that this is a part of the ICANN Web site that relates to the “domain name system” in its “frequently asked questions” folder. Not all Web site operators will make the file structure information available to users. What is more important than the file structure of a Web page, however, is the letters following the server information. In the above example, the suffix of the domain name is “.org.” This is an

server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function.


14. CAPRON & JOHNSON, supra note 6, at 562 (demonstrating that the World Wide Web is a subset of sites on the Internet with text, images, and sounds accessed via graphical user interfaces).

example of a generic Top-Level Domain ("gTLD"), connoting that the operator of the Web site is an organization. The most popular gTLDs, at least on a commercial level, are "_.com," "_.org," and "_.net." That is because these names connote organizations or business operations, and are not tied to any particular geographical location, so they appear to be more global or universal than domain names suffixed by a country-code Top-Level Domain ("ccTLD"), such as "_.uk" for the United Kingdom, "_.ca" for Canada, and "_.au" for Australia.¹⁶

There are many other forms of gTLDs that are not country-specific. They include "_.edu," which is used predominantly for educational institutions, and "_.gov," which is used for governmental departments. In November 2000, ICANN released seven new gTLDs because of concerns that the existing gTLDs were being exhausted and that alternatives were not available for people and businesses who needed them.¹⁷ Some of the new gTLDs were specific to a particular area of operation and some were more general.¹⁸ The new gTLDs are: "_.aero," for the aviation community; "_.biz," for business purposes; "_.coop," for cooperatives; "_.info," for general, unrestricted use; "_.museum," for museums; "_.name," for personal names; and "_.pro," for professionals.¹⁹

Additionally, as noted above, the domain name system caters to ccTLDs. Many businesses use country-code specific top-level domains, or have more than one Web site, including a country-code specific Web site and a more generic Web site. An obvious example is Amazon.com, Inc., which, in addition to its namesake Web site, boasts an amazon.co.uk site for the United Kingdom, an amazon.de site for Germany, an amazon.fr site for France, an amazon.co.jp site for Japan, and an amazon.ca site for Canada.²⁰

¹⁷. ICANN, Top-Level Domains (gTLDs), at http://www.icann.org/tlds (last modified Dec. 16, 2003).
¹⁸. See id.
²⁰. WHOIS, Query Result, at http://195.66.240.211/cgi-bin/whois.cgi?query=amazon.co.uk&x=7&y=12 (last visited Nov. 22, 2005); DENIC, Domain Query—Results, at http://www.denic.de/en/whois/data.jsp (last updated Aug. 25, 2004) (displaying Amazon as the domain holder when "amazon" is entered in the domain query search field); AFNIC, WHOIS, at http://www.afnic.fr/outils/whois (last visited Nov. 22, 2005) (displaying Amazon as the domain holder when "amazon.fr" is entered in the nom de domaine search field); !JP, WHOIS, at http://whois.jprs.jp/en (last updated Dec. 1, 2004) (displaying Amazon as the domain holder when "amazon.co.jp" is entered in the whois search keyword field); Canadian Internet Registry Authority, Information on
Herein lies one of the problems of the domain name system from the “competing interests” perspective: nothing in the domain name system prevents one corporation from monopolizing various forms of a particular domain name. This may or may not be problematic where there is only one party with a likely interest in a particular name. However, where more than one party might have competing interests in the same name, a system that allows for the monopolization of multiple versions of the name by one entity can create problems. If Amazon.com can hold all the above-listed domain names as well as adding new country code versions of its name and perhaps even new generic versions of its name, such as amazon.net or amazon.biz, does this cause a problem for other entities with objectively legitimate interests in maintaining a Web site with “amazon” in the domain name?

III. THE CURRENT LEGAL AND REGULATORY FRAMEWORK FOR INTERNET DOMAIN NAME DISPUTES

A. Domain Names and Trademark Policy

The current approaches to Internet domain name disputes focus on protecting holders of trademarks from bad-faith registrations and uses of domain names that correspond to relevant trademark interests. In some senses, this is an unusual extension of trademark policy into a new area of legal regulation. This development is remarkable because traditional trademark law and policy is aimed at preventing consumer confusion about the source and, to some extent, the quality of particular goods or services. More recently, trademark legislation has been utilized to protect famous trademarks against dilution. The idea of importing a notion of bad

---

2005] DOMAIN NAME DISPUTES 1369


21. In fact, a recent report by the World Intellectual Property Organization (“WIPO”) shows that the new gTLDs with little to no registration restrictions had the most number of “repeat registrants” and the lowest number of new registrants, suggesting that a large number of new domain names were registered defensively by people who already held corresponding domain names in other gTLD spaces such as “.com,” “.org,” or “.net.” New Generic Top-Level Domains, supra note 5, ¶ 21.

22. Amazon.com has already registered amazon.biz and mapped that domain name on to the IP address for the amazon.com Web site. .BIZ Registry, WHOIS Data, at http://www.whois.biz/whois.cgi?TLD=biz&dn=amazon&TYPE=DOMAIN&Search=Submit+Query (last visited Nov. 22, 2005).


24. 15 U.S.C. § 1125(c) (providing the definition of “dilution” from the Federal Trademark Dilution Act of 1995); GILSON, supra note 23, § 5A.01 (detailing the new federal trademark dilution legislation of 1995).
faith into trademark policy as the basis for a cause of action in the "cyberpiracy" context has been a more recent development. It is largely an outgrowth of early Internet domain name disputes in which bad-faith registration of a domain name seemed a significant factor taken into account by courts in holding that a particular domain name registration or use amounted to a trademark infringement.\footnote{25. Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1324-25 (9th Cir. 1998) [hereinafter Panavision III].}

Consider, for example, the now famous—or infamous—litigation involving "cyber-pirate" Dennis Toeppen's multiple registrations of Internet domain names corresponding to famous corporate trademarks in the early days of the Internet.\footnote{26. See infra notes 28-29 and accompanying text.} Trademark infringement holdings against Toeppen seemed to be based as much on courts being convinced that Toeppen's actions were morally wrong as on the application of trademark law to the facts. Judges were prepared to hold that Toeppen's offers to sell the relevant domain names to the "rightful" owners were commercial uses of trademarks despite the fact that such activities were not the kinds of commercial uses traditionally associated with trademark law as the basis for a successful infringement action.\footnote{27. 15 U.S.C. § 1125(c)(1) (requiring "commercial use" of a mark for a trademark dilution action); id. § 1125(c)(4)(B) (preventing a successful trademark dilution action if the defendant has only made a noncommercial use of the relevant mark).}

The language of some of these judgments suggests significant concern with immoral or bad-faith activities involving domain names, regardless of how well the facts of a given case fit the traditional trademark infringement model. In \textit{Panavision International, L.P. v. Toeppen},\footnote{28. 141 F.3d 1316.} for example, Judge Thompson stated that:

\begin{quote}
[Toeppen's] use [of the relevant marks] is not as benign as he suggests. Toeppen's "business" is to register trademarks as domain names and then sell them to the rightful trademark owners. He "act[s] as a 'spoiler,' preventing Panavision and others from doing business on the Internet under their trademarked names unless they pay his fee.\footnote{29. Id. at 1325 (quoting \textit{Panavision I}, 938 F. Supp 616, 619 (C.D. Cal. 1996)). See also Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1239 (N.D. Ill. 1996) (making similar observations about Toeppen's cybersquatting conduct amounting to a "commercial use" of the relevant mark for the purposes of trademark law).}]
\end{quote}

There is an obvious concern here with benign uses of marks versus
bad-faith uses. The plaintiffs are regarded as "rightful" owners of the trademarks, which is unquestionable. However, little judicial thought is given to whether those rightful owners of the marks should also be rightful owners of corresponding domain names.

As a result of growing judicial, corporate, and legislative concern about bad-faith registrations of Internet domain names in the early- to mid-1990s, action was taken at both the international and domestic levels to create domain name dispute resolution procedures that would protect trademark holders against such bad-faith registrations. These procedures were aimed at protecting trademark holders against activities such as those conducted by Toeppen in the mid-1990s. Thus, they are somewhat narrow in their scope and, even though they protect trademark holders against certain bad-faith conduct, they are in some ways outside of traditional trademark policy. They do not necessarily prevent consumer confusion or trademark dilution in the traditional trademark sense, but rather preserve commercial property interests in trademarks against bad-faith cybersquatting activities.

This has led to some difficulties of application and interpretation in cases that are not traditional cybersquatting situations. In some ways, standard cybersquatting activities are the "easy cases," once the legal and regulatory system has identified them as a legal wrong. However, other forms of Internet domain name disputes are more problematic. This Article focuses on identifying and categorizing those other forms of Internet domain name disputes that have been emerging in recent years as difficult cases under the new forms of domain name dispute resolution. It further suggests new approaches to resolving these emerging categories of domain name disputes on the basis of perceived social and cultural values in the global information age. However, before categorizing these forms of disputes, it is worth briefly surveying the current approaches to domain name dispute resolution.

B. Uniform Domain-Name Dispute-Resolution Policy

The main source of dispute resolution rules that apply to domain names is the Uniform Domain-Name Dispute-Resolution Policy, promulgated by ICANN. The UDRP is a form of private

---

30. *Panavision II*, 141 F.3d at 1325.
31. *See supra* notes 2-3 and accompanying text.
32. *See supra* notes 4-5 and accompanying text.
33. For example, in the *Panavision* case, Toeppen had posted aerial photos of the town of Pana, Illinois, on the relevant Web site, which would, by itself, be unlikely to cause any consumer confusion, although it is arguable that it might dilute the Panavision trademark. *Panavision II*, 141 F.3d at 1325.
34. *See UDRP,* supra note 3.
regulation that is implemented through various organizations accredited by ICANN, the most significant of which is the World Intellectual Property Organization ("WIPO").\textsuperscript{35} The UDRP is a private, international, inexpensive,\textsuperscript{36} relatively fast, and predominantly online\textsuperscript{37} dispute resolution procedure for situations in which a complainant is disputing the registration of a domain name. The UDRP does not oust the jurisdiction of national courts.\textsuperscript{38} However, all domain name registrants are contractually bound to submit to a mandatory arbitration under the UDRP if a complaint is made under the UDRP about the registration of one or more relevant domain names.\textsuperscript{39} This dispute is managed by arbitrators licensed by one of the organizations charged with hearing disputes under the UDRP.\textsuperscript{40} It involves the receipt of a complaint and a response by the registrant.\textsuperscript{41} The arbitrator or panel then provides a decision and resolution based on this material.\textsuperscript{42} There are generally no in-person hearings.\textsuperscript{43} The only orders that can be made under the UDRP are orders for cancellation of a disputed name or for transfer of a domain name to the complainant.\textsuperscript{44}

The grounds on which a decision is made under the UDRP are based on commercial considerations that largely resemble some of the key elements of trademark law, as well as the bad-faith concerns identified above in relation to domain name registration.\textsuperscript{45} Complaints under the UDRP mechanism generally must relate to a domain name registered in a way that misuses a registered trademark or service mark.\textsuperscript{46} A complaint must be made on the

\begin{itemize}
\item \textsuperscript{35} World Intellectual Property Organization, \textit{Domain Name Dispute Resolution Resources}, at http://arbiter.wipo.int/domains/resources/index.html (last visited Nov. 22, 2005).
\item \textsuperscript{38} See UDRP, supra note 3, §§ 3(b), 4(k).
\item \textsuperscript{39} Id. § 4. The UDRP is incorporated by reference into domain name registration agreements. See id. § 1.
\item \textsuperscript{40} See Rules for UDRP, supra note 37, §§ 1, 6.
\item \textsuperscript{41} Id. §§ 3(a), 4(a), 5(a).
\item \textsuperscript{42} Id. § 15.
\item \textsuperscript{43} Id. § 13 ("There shall be no in-person hearings (including hearings by teleconference, videoconference, and [Web conference], unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.").
\item \textsuperscript{44} Id. § 4(i).
\item \textsuperscript{45} See supra notes 25-33 and accompanying text.
\item \textsuperscript{46} See UDRP, supra note 3, § 4(a)-(c).
\end{itemize}
basis of the three grounds set out in Paragraph 4(a) of the UDRP:

(i) [that the disputed] domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) [that the registrant has] no rights or legitimate interests in respect of the domain name; and

(iii) [that the] domain name has been registered and is being used in bad faith.\(^47\)

The UDRP provides guidance about how a registrant can demonstrate rights or legitimate interests in a domain name in response to an arbitration claim,\(^48\) and also about what evidence a complainant might bring to support an allegation that the registrant is using the name in bad faith.\(^49\) With respect to the former, the UDRP sets out some factors that a registrant may use to demonstrate a legitimate interest in a disputed domain name. In particular she might show that:

(i) before any notice to [her] of the dispute, [she had] use of, or [made] demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) [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 [in the name]; or

(iii) [she is] making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert customers or to tarnish the trademark or service mark at issue.\(^50\)

This is an inclusive list; an arbitrator or panel might consider other evidence presented to support an argument that the registrant has a legitimate interest in the domain name in question.\(^51\) However, the list as it stands is obviously focused on the protection

---

47. Id. § 4(a)(i)-(iii).
48. See id. § 4(c).
49. See id. § 4(b).
50. Id. § 4(c)(i)-(iii).
51. See id. § 4(c).
of trademark rights and related interests in commerce, rather than protecting any other interests.

In terms of evidence of bad-faith use, the UDRP includes a non-exclusive list of factors that might indicate a bad-faith use of a domain name. These are based largely on concerns about cybersquatting that arose in the early to mid-1990s. The bad-faith factors set out in the UDRP relate to the claimant establishing:

(i) circumstances indicating that [she has] registered or acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant, [where the complainant] is the owner of the trademark or service mark, or to a competitor of the complainant, for valuable consideration . . . ; or

(ii) [that the registrant has] 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 [the registrant has] engaged in a pattern of such conduct; or

(iii) [that the registrant has] registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) [that,] by using the domain name, [the registrant has] intentionally attempted to attract, for commercial gain, Internet users to [the registrant’s] Web site . . . by creating a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement of [the registrant’s] Web site or location or of a product or service [available on that] Web site or location.

Again, we see the concept of bad faith linked with traditional trademark and unfair-competition-law principles. Some of the UDRP’s bad-faith factors relate clearly to cybersquatting activities, while others reflect more traditional trademark concerns, such as the prevention of consumer confusion. Various assumptions have been made in drafting the UDRP in terms of the values that should be promoted on the Internet, at least in terms of domain name registration. The overriding emphasis is clearly on the protection of

52. See id. § 4(b).
53. Id. § 4(b)(i)-(iv).
54. See id.
Western commercial trademark interests, presumably in an attempt to avoid chilling the development of electronic commerce over the Internet.

However, there is no reason that the UDRP or any other set of rules and regulations governing competing interests in Internet domain names needs to be focused so sharply on protecting trademarks, although, presumably, those principles should play some role in domain name governance. Why, for example, is there an assumption that trademark rights are more important with respect to domain names than are individuals' rights to use their own personal names as domain names or the rights of cultural groups to use geographical identifiers or other culturally significant words? Presumably this is because Western government policy has been more concerned with protecting and promoting the development of electronic commerce in recent years than in promoting other values on the Internet.

Even if the view is taken that government policies should focus on protecting the development of electronic commerce above other interests on the Internet, is it necessarily true that the most efficient way to do that is through applying modified trademark and unfair-competition-law principles to the Internet? Consider, for example, the bad-faith factors from the UDRP, as well as the Toeppen litigation described above. The UDRP clearly contemplates that a person who has trademark rights corresponding to a registered domain name also has the right to prevent cybersquatting activities. In other words, the trademark holder

55. See id. § 4(a)-(c).
56. It is noteworthy that the UDRP envisages that the assertion of a legitimate interest in a domain name corresponding to a personal name is effectively a defense to a UDRP arbitration proceeding. Id. § 4(c)(iii). However, there is no right to bring a complaint under the UDRP based on a right in a personal name corresponding to a given domain name. See infra note 80 and accompanying text. More recently, ICANN introduced the “.name” gTLD partly as an alternative domain space for registering interests in personal names. However, this domain space has not proved as popular as “.com,” even for many personal names. There have certainly been very few disputes involving “.name” domain names. New Generic Top-Level Domains, supra note 5, ¶ 103.
57. See Chander, supra note 9, at 717.
59. See supra notes 25-33, 52-53 and accompanying text.
60. See UDRP, supra note 3, § 4(a)-(b).
should be able to prevent another person from registering a domain name corresponding to her trademark in order to sell it to her or one of her competitors for a profit.

There is clearly an underlying assumption here that cybersquatting is a dishonest and unfair activity and should be discouraged. But is this a valid assumption? Can it be empirically proven that it is not, in fact, more efficient to allow cybersquatting and let the market sort itself out in terms of who eventually gains access to particular domain names? Presumably, a cybersquatter will not be able to sell a domain name to an organization with a corresponding trademark at a price that is greater than the domain name is worth to the organization. Thus, is it not possible that an efficient market in domain names would arise in the commercial arena without any form of regulation or, alternatively, with a form of regulation that generally allows cybersquatting when it appears to be economically efficient but limits or restricts such activities if they are causing market disruption? Under such regulation, a cybersquatter would be forbidden from holding domain names hostage for exorbitant prices, rather than selling them to the “rightful” owners for reasonable market values.

Such a model could be derived from ideas underlying government-monitored compulsory licensing schemes found in some countries' patent legislation. Under such a scheme, the government would intervene where the market is unable to come to a socially and economically beneficial solution. Of course, the obvious counterargument is that there is no social value in encouraging these cybersquatting activities and, as a result, there is no good reason to allow such markets to develop. Nevertheless, analogies may be made with the physical world of land ownership where property speculators buy land with little worth for them, aside from the potential that it will be more valuable in the hands of another who may want to purchase it for a significantly higher price. Is there any reason to regulate differently in the virtual world of domain name registrations?

In any event, there are other, less clear-cut variations on this theme. An obvious example of a more complicated situation is that in which two or more people or businesses each have legitimate commercial interests in a particular domain name. If one of them has registered the name, but it is worth more to one of the other corresponding trademark holders, is it not possible that market

---


62. See generally Nguyen, supra note 9, at 60 (suggesting that the “secondary market for domain names often has been compared to real estate speculation”).
forces will determine who ultimately gets to use the domain name? Presumably, the person to whom it is worth the most will pay that price to obtain the name from the registrant without any specific regulation. This type of situation is not well catered for under the UDRP as currently drafted. The UDRP operates under the assumption that a domain name should be cancelled or transferred in circumstances when one person has a legitimate interest in the domain name based on a corresponding trademark or service mark and another person has registered or used the name in bad faith. That paradigm does not cover the situation in which two or more organizations have competing legitimate interests in the same domain name. This is an obvious example of the current system's limitations with respect to resolving domain name disputes even within the purely commercial trademark context.

C. Anticybersquatting Consumer Protection Act

Around the time that the UDRP was implemented, Congress enacted the Anticybersquatting Consumer Protection Act of 1999. This legislation added provisions to the Lanham Act in order to protect domain names that correspond to a registered trademark against bad-faith registrations. Like the UDRP, this legislation was ratified in response to concerns about cybersquatting activities such as those conducted by Dennis Toeppen. It is arguable whether the ACPA actually adds anything substantial to domestic trademark law, given that judges were already prepared to find that cybersquatting constituted a "commercial use" of a trademark, as required for a trademark infringement action under the Lanham Act. However, it does potentially streamline legal proceedings involving domain names and adds further protections for domain names corresponding to personal names.

The ACPA establishes a civil action against a person who registers, traffics in, or uses a domain name corresponding to a trademark with a bad-faith intent to profit from the mark. For these purposes, a "personal name which is protected as a mark" is

63. See discussion infra Part IV.D.
64. UDRP, supra note 3, § 4(a)-(b), (i).
65. See id. § 4(c).
67. Id. §§ 1051-1141.
68. Id. § 1125(d)(1)(A).
69. See supra notes 4-5 and accompanying text.
70. See Panavision II, 141 F.3d 1316, 1324-25 (9th Cir. 1998); see also Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1239 (N.D. Ill. 1996).
72. Id. § 1125(d)(1).
included in the concept of trademark.\textsuperscript{73} Bad faith is defined in terms that relate to knowing and unauthorized incursions into a complainant’s trademark rights that correspond to the domain name.\textsuperscript{74} A defense may be mounted if the defendant “believed and had reasonable grounds to believe that [her] use of the domain name was a fair use [under American trademark law] or was otherwise lawful.”\textsuperscript{75} In terms of remedies, the ACPA empowers a court to “order the forfeiture or cancellation of [a] domain name or the transfer of [a] domain name to the owner of [a relevant trademark].”\textsuperscript{76}

With respect to any bad-faith intent to profit from a trademark by using a domain name, the ACPA takes an approach similar to the UDRP’s bad-faith test, in setting out an inclusive list of factors that may be taken into account by a court to determine bad faith.\textsuperscript{77} As with the UDRP bad-faith factors, the ACPA bad-faith factors rely significantly on assumptions about the immorality of cybersquatting. The bad-faith factors in the ACPA, though,

\begin{itemize}
  \item [(I)] the trademark or other intellectual property rights of the defendant, if any, in the domain name;
  \item [(II)] the extent to which the domain name consists of the legal name of the defendant or a name that is otherwise commonly used to identify the defendant;
  \item [(III)] the defendant’s prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
  \item [(IV)] the defendant’s bona fide noncommercial or fair use of the trademark in a Website accessible under the domain name;
  \item [(V)] the defendant’s intent to divert consumers from the trademark owner’s online location to a Website accessible under the domain name that could harm the goodwill represented by the trademark, either for commercial gain or with intent to tarnish or disparage the trademark;
  \item [(VI)] the defendant’s offer to transfer . . . the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the defendant’s prior conduct indicating a pattern of such conduct;
  \item [(VII)] the defendant’s provisions of material and misleading false contact information when applying for the registration of the domain name, the defendant’s intentional failure to maintain accurate contact information, or the defendant’s prior conduct indicating a pattern of such conduct; and
  \item [(VIII)] the defendant’s registration or acquisition of multiple domain names which the defendant knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names . . . .
\end{itemize}

\textit{Id.} § 1125(d)(1)(B)(i)(I)—(VIII).

\begin{itemize}
  \item \textsuperscript{73} \textit{Id.} §§ 1125(d)(1)(A), 1129.
  \item \textsuperscript{74} \textit{Id.} § 1125(d)(1)(B)(i).
  \item \textsuperscript{75} \textit{Id.} § 1125(d)(1)(B)(ii).
  \item \textsuperscript{76} \textit{Id.} § 1125(d)(1)(C).
  \item \textsuperscript{77} This list of bad-faith factors includes:
    \begin{itemize}
      \item [(I)] the trademark or other intellectual property rights of the defendant, if any, in the domain name;
      \item [(II)] the extent to which the domain name consists of the legal name of the defendant or a name that is otherwise commonly used to identify the defendant;
      \item [(III)] the defendant’s prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
      \item [(IV)] the defendant’s bona fide noncommercial or fair use of the trademark in a Website accessible under the domain name;
      \item [(V)] the defendant’s intent to divert consumers from the trademark owner’s online location to a Website accessible under the domain name that could harm the goodwill represented by the trademark, either for commercial gain or with intent to tarnish or disparage the trademark;
      \item [(VI)] the defendant’s offer to transfer . . . the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the defendant’s prior conduct indicating a pattern of such conduct;
      \item [(VII)] the defendant’s provisions of material and misleading false contact information when applying for the registration of the domain name, the defendant’s intentional failure to maintain accurate contact information, or the defendant’s prior conduct indicating a pattern of such conduct; and
      \item [(VIII)] the defendant’s registration or acquisition of multiple domain names which the defendant knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names . . . .
    \end{itemize}
\end{itemize}
contemplate additional protection for a defendant's right to use her personal name as it may be incorporated into a domain name. This factor is not necessarily determinative in a given case but is just one item that may be taken into account by a court.

Furthermore, personal names receive specific protection under section 1129(1)(A), which states that:

Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.

This provision allows personal names to be used as the basis of a complaint under the ACPA in a manner not contemplated in the UDRP. However, there may be some question as to whether such a provision rightfully belongs in the ACPA, particularly as it apparently covers personal names that are not utilized for commercial trademark purposes. Once again, emerging domain name policy is blurring the boundaries of traditional trademark law.

The ACPA includes some additional bad-faith factors that are not expressly contemplated in the UDRP, such as the defendant's failure to provide or maintain accurate contact information in a domain name registry, which is seen as potential evidence of a bad-faith intent to profit from a trademark corresponding to a domain name. The ACPA also expressly suggests that the practice of registering multiple domain names that correspond to existing trademarks might be evidence of bad faith. Again, this is based on the assumption that such conduct deserves to be prohibited.

With respect to personal names, despite the provisions of section 1129(1)(A) of the ACPA, it is not clear that society has reached the point where individuals are prepared, or even aware of their right, to litigate to protect their personal names when those names do not correspond to commercially valuable trademarks. In fact, many such individuals may not have the financial resources to avail themselves of these provisions in a courtroom. Additionally,

78. Id. § 1125(d)(1)(B)(ii)(II).
79. Id. § 1129(1)(A).
80. The UDRP only contemplates personal names being used to establish a legitimate interest in a domain name by way of a defense to a UDRP complaint. UDRP, supra note 3, § 4(c)(ii). There is no right to bring a complaint under the UDRP based on a right in a personal name that corresponds to a given domain name. Id. § 4(a)(ii), (c)(ii).
82. Id. § 1125(d)(1)(B)(i)(VIII).
this remedy may only be available to people who live in, or have some significant connection with, the United States. In any event, the ACPA does not protect any other interests in domain names—such as a cultural group's interest in a domain name corresponding to a geographical place or a religious icon. Overall, the ACPA's approach to cybersquatting largely mirrors that of the UDRP. Both are skewed in favor of protecting Western-style commercial trademark interests against various kinds of bad-faith incursions.

If a broader global policy on domain name rights and interests is to be developed in the future, any domestic legislation would have to mirror the terms of such a policy or, at least, not significantly contradict the policy. If individual jurisdictions are encouraged to legislate independently of each other for various issues involving domain names, an unworkable patchwork could ensue of laws which are not globally harmonized among nations or even, in federal states, nationally harmonized among political subdivisions. The recent interest in state-based laws relating to "political cybersquatting" in the United States may be an emerging example of such failure to create a harmonized approach to disputes involving personal names in cyberspace where the UDRP and the ACPA fall short of resolving the relevant disputes.

Now may be a good time for the global community to start identifying interests in domain names, other than commercial trademark interests, that may need to be protected in cyberspace in the future. It would certainly be preferable if global attention were paid to this issue and thought were given to a harmonized approach to resolving relevant disputes, rather than leaving the issues for piecemeal and potentially contradictory or disharmonized national regulation. It may not be a particularly difficult task to identify the kinds of interests that would need to be taken into account in developing a new global policy for Internet domain names, as some of the more salient issues are currently arising in disputes arbitrated under the UDRP and argued in domestic courts under trademark law, including the ACPA.

It seems that the disputes currently arising under the UDRP and the ACPA are beginning to point the way to the kinds of

87. See discussion infra Part IV.C-F.
balancing exercises that will need to be conducted in the future in relation to domain name policy. Many of these disputes evidence distinctly different concerns to the original problem of protecting trademark holders against bad-faith cybersquatters. Some of the more salient classes of disputes are examined below. This discussion highlights the shortcomings of the existing dispute resolution models in resolving these disputes. It also suggests new approaches to resolving these various different classes of disputes, based on an attempt to cater to emerging social, cultural, and economic values in the global information age. This may ultimately lead to a more workable global system based on social and cultural expectations of Internet usage.

IV. CATEGORIZING DOMAIN NAME DISPUTES AND APPROPRIATE REMEDIES

A. Crafting a Domain Name Dispute Classification Scheme

One reason for advocating an expanded approach to domain name dispute resolution policy is that an approach based predominantly on protecting commercial trademarks against cybersquatters has a number of shortcomings. This has become obvious in the disputes that have come before courts and UDRP arbitrators in recent years. Additionally, the current system may prevent adequate consideration of matters that do not readily translate into ACPA or UDRP terms because of implicit assumptions in those systems about who has "better" rights in domain names. For example, now that the idea of domain names as trademark equivalents has taken hold, those who might otherwise have asserted an interest in a domain name because, for example, it corresponds to their personal name or a cultural interest, might now choose not to bother. They may simply assume that they do not, and are not intended to, have any legal entitlements to the relevant domain name.

Domain name disputes currently come in many different forms, and the following discussion might not consider all possible permutations and combinations of interests that could arise in relation to a domain name. However, it does address a variety of different kinds of domain name disputes that have arisen in recent years, some of which clearly fit more neatly within traditional trademark or unfair-competition paradigms than others. Drawing from the recent history of domain name disputes, it is possible to

88. See, e.g., infra Part IV.D.
89. See, e.g., infra Part IV.E.2 (discussing the domain name dispute arising out of Kathleen Kennedy Townsend's 2002 Maryland gubernatorial campaign).
suggest a new classification scheme for such disputes as follows. This scheme evidences the fact that the cybersquatting cases catered for in the ACPA and the UDRP only make up a small proportion of the overall number of potential disputes. The classes of disputes identified below also clearly lend themselves to new practical approaches to dispute resolution as detailed in the following discussion. Domain name disputes that have arisen in recent years might be classified as follows.

(1) "Classic" Cybersquatting: This category of disputes covers situations in which a person has registered one or more domain names that correspond to well-known trademarks with a view to commercial profit by offering to transfer the domain name(s) to a party interested in the trademark for valuable consideration. This has been considered a bad-faith practice and has been relatively successfully regulated by the ACPA and the UDRP since 1999, as detailed above. Thus, the following discussion does not deal in any detail with new approaches to this class of disputes as compared with the other classes set out below.

(2) "Noncommercial" Cybersquatting: This category refers to situations in which a person has registered usually only one domain name, but possibly more, for a predominantly noncommercial purpose. An obvious example might be where a person has registered a domain name corresponding to another person’s trademark in order to use the domain name in a Web site that comments on the activities of the trademark holder. Recent examples in the United States have involved registrations of a domain name corresponding to the Planned Parenthood trademark, the People for the Ethical Treatment of Animals ("PETA") trademark, and the Bosley Medical Institute trademark.
Such conduct is perhaps not truly cybersquatting in the "classic" sense of the term, because the registrant is actually using the name herself for a particular purpose—commentary, parody, etc.—rather than for purposes of extorting money from a person with an interest in a corresponding trademark. This may, or may not, justify separate treatment in the dispute resolution arena than "classic" cybersquatting cases, depending on the circumstances.

"Noncommercial" in this context is not a term of art. A person who registers a domain name with a purpose of making commentary on a particular issue may have a secondary purpose of commercial profit, as the following discussion demonstrates. This category of disputes might more appropriately be referred to as "First Amendment Cybersquatting" or something similar. However, the "noncommercial" label has been applied here with the aim of encompassing a potentially broader class of cases than just free speech cases.96

(3) Contest between Multiple Legitimate Interests: This category covers situations in which two or more people have what might be called a "legitimate" interest in the same domain name, which would occur, for example, when two or more companies have a similar trademark that corresponds with a particular domain name.97 Thus, it encompasses those situations where multiple legitimate interest holders are competing for the same domain name.

(4) Disputes Involving Personal Names: This category of disputes may be further subcategorized into: (i) disputes involving celebrity names (for example, actors, musicians, sports stars, etc.);98 (ii) disputes involving politician names;99 and (iii) disputes involving names of private individuals.100 These issues come in different flavors. A number of recent examples are provided below.

(5) Culturally Significant Names, Geographical Locators, etc.: This is a somewhat miscellaneous category of disputes for which

96. An obvious example might be Joshua Quittner's registration of the mcdonalds.com domain name in the early days of the domain name system. See infra Part IV.C.5. This case was never actually litigated and it may or may not truly be classified as a free speech issue. The purpose of the registration here was to demonstrate the workings of the domain name system in the early days of the Internet and the fact that many corporations had not yet appreciated how commercially valuable and important it would be to them to register domain names corresponding to their commercial trademarks. See infra notes 193-98 and accompanying text. On the other hand, the scenario might be classified as a First Amendment case because the registrant was a journalist writing a story about Internet domain names and their commercial value. See infra note 199 and accompanying text.

97. See, e.g., infra Parts IV.D.1, IV.D.3 (discussing the delta.com and clue.com situations as examples of competing legitimate interests in the same domain name).

98. See infra Part IV.E.1.

99. See infra Part IV.E.2.

100. See infra Part IV.E.3.
there may be little data in records of existing arbitrations and litigation, at least in comparison to the other classes of disputes identified above. This category of disputes contemplates some of the issues recently addressed by Professor Chander in terms of the failure of the current system to take into account cultural and often noncommercial interests in domain names such as geographical place names or culturally significant words and phrases. 101 WIPO has also recently made some suggestions on future developments in this area.102

This list of dispute classes is not necessarily exhaustive, although it does capture the essence of the kind of classification scheme that could be developed for domain name disputes in order to ensure that Internet regulation does more than just protect commercial trademark interests. There are several classes of disputes that are not included here. In particular, certain types of disputes have been intentionally omitted from this categorization because they do not necessarily add anything to the points being made here about the need to create a more nuanced approach to domain name disputes outside the protection of trademark interests against bad-faith cybersquatters.

One category omitted above includes those disputes involving a deliberate misspelling of a trademark or a person's name in a registered domain name. If, for example, a person wanted to confuse the customers of Microsoft Corporation, in the trademark sense of "confusion," she might register a deliberate misspelling of microsoft.com, such as microsfot.com, in the hope of attracting customers to a competing Web site or in order to make commentary about, or parody of, the activities of Microsoft.103 These kinds of cases do not add much to the above classification scheme because deliberate misspelling situations can arise within all of these classifications as a subset of the behavior under consideration. The

101. Chander, supra note 9, at 718.
103. In fact, a company called Zero Micro Software did, at one stage, register the domain name micros0ft.com (with a zero in place of the second "o"), but the registration was suspended after Microsoft filed a protest with the registering authority. The domain name was ultimately abandoned for nonpayment of fees and was later registered to someone else. Bitlaw: A Resource on Technology Law, Domain Name Disputes (2000), at http://www.bitlaw.com/internet/domain.html (last visited Nov. 22, 2005) [hereinafter Bitlaw]. At the time of this writing, the micros0ft.com name is still registered, but the Web site only contains some random alpha-numeric characters on a blank background. See http://www.micros0ft.com (last visited Nov. 22, 2005).
deliberate misspelling approach is just another way to achieve any of the ends identified within each of the above classifications. Examples include confusing customers as to the source or origin of goods or services, making commentary or parody about an existing trademark holder, confusing consumers about whether a celebrity or politician has endorsed product lines available on a Web site or otherwise making comments about such a person, and confusing people about the political message of a particular politician.  

Another kind of domain name dispute purposely omitted from the above discussion is that which relates to the unauthorized use of a trademark or personal name, or a deliberate misspelling of a trademark or personal name, in the broader URL of a Web site. In these cases, the disputed appellation is not the registered domain name of the relevant Web site per se, but rather appears in conjunction with the domain name as part of the Web site's URL. An example is www.compupix.com/ballysucks, which was the subject of litigation in the case of Bally Total Fitness Holding Corporation v. Faber. The problem in that case was not that the registrant had registered a domain name corresponding to the plaintiff's registered trademark. If he had done so, the domain name would have looked something like bally.com or perhaps ballysucks.com. Rather, the litigation involved a domain name that did not correspond to the plaintiff's trademark, compupix.com, but that happened to reference a sub-page on the relevant Web site that criticized Bally's operations and that appeared under the composite URL described above.

104. If a label is needed for these kinds of situations, it would be possible to describe them as "typo-squatting" situations. Typo-squatting could occur within any of the categories described above as a subcategory of that particular class of dispute. I am indebted to Professor Chander for suggesting this term.

105. 29 F. Supp. 2d 1161, 1162 (C.D. Cal. 1998).

106. This domain name is actually registered to Bally Shoe Factories Ltd. See Bally Shoe Factories Ltd., at http://www.bally.com (last visited Nov. 22, 2005).


108. Bally, 29 F. Supp. 2d. at 1162. As a matter of interest, as of the date of this writing, the defendant in Bally appeared to have succeeded in convincing the district court that the use of Bally's trademark within the URL, with reference to Web content critical of Bally Total Fitness on the relevant Web site, was not a trademark infringement under the Lanham Act. Id. at 1163-64. However, the disputed sub-page of the Web site has since been removed from www.compupix.com. This Web site predominantly contains adult-oriented photography of male figures aimed at the homosexual community. See http://
These disputes are not discussed here because they do not relate to rights in domain names per se but, rather, to uses of Web pages and URLs that incorporate commercially valuable trademarks without authorization. Important Internet-age applications of trademark laws arise in these cases, but they do not directly bear on a consideration of the extent to which the domain name system per se might be expanded in scope to better accommodate competing interests in domain names.

This discussion also does not deal with the area of disputes involving metatags and Internet search engines as they may implicate trademark law. This has been an emerging area of American trademark jurisprudence in recent years because of the development of various practices with respect to search engine technology. In the early days of this technology, many search engines utilized metatags to find Web pages for listing in response to an Internet search. Web site operators could insert these metatags into their Web page structures in order for the search engines to pick them up and prioritize them among search results. Sometimes, a Web site operator might use a competitor's domain name or trademark as a metatag on its own site, causing its Web page to be more prominently displayed in search results and thereby allowing it to attract customers away from the competitor. For example, a software manufacturer in competition with Microsoft Corporation could use the microsoft.com domain name or, alternatively, the word "microsoft" itself not as a domain name, but as a metatag on its own Web site, in the hope that its Web site would be prioritized in an Internet search for the word "microsoft."

109. See Brookfield Communications v. West Coast Entm't Corp., 174 F.3d 1036 (9th Cir. 1999) (adjudicating a complaint in which the defendant used the plaintiff's domain name in the defendant's metatags to draw customers to its Web site); Playboy Enters., Inc. v. Terri Welles, Inc., 78 F. Supp. 2d 1066 (S.D. Cal. 1999), aff'd in part and rev'd in part 279 F.3d 796, 807 (9th Cir. 2002) (holding that the defendant was entitled to use the Playboy trademark in metatag for the defendant's Web site to enable potential customers to locate the Web site more easily).


111. Rajzer, supra note 110, at 438.

112. Id. at 439.

113. This is, perhaps, not the best example because most people looking for the Microsoft Corporation Web site would guess that its domain name was
More problematic in recent years have been deals between advertisers and search engine operators to prioritize certain Web pages in search results in return for valuable consideration. Thus, organizations with lesser-known trademarks and domain names may be at a disadvantage in terms of search engine results if they do not pay search engine operators to have their pages prioritized when a user enters certain relevant search terms. These disputes are very interesting and raise new issues for trademark law in particular. However, they also do not directly involve considerations about reworking the domain name system in the manner proposed here.

Finally, the following discussion considers each of the categories of disputes identified above in isolation from the other categories, despite the fact that disputes involving more than two parties may involve more than one category. An example of such a case would be a tripartite dispute involving a legitimate trademark holder, a bad-faith cybersquatter, and an individual whose personal name happened to correspond to the domain name in question. This dispute would clearly evidence an overlap of the “classic” cybersquatting category with the personal name category. In fact, even a bipartite dispute between a corporation and an individual relating to the use of a domain name that happens to correspond to both a personal name and a trademark might evidence such an overlap.

This Article does not try to establish priority rules for such cases. What is suggested, instead, is that alternative approaches to remedial measures may be developed that might lessen the need for developing priority rules between classes of disputes. Domain name sharing, for example, is a strategy discussed below that might encourage people and groups with different interests in the same domain name to share a home page containing links to their individual Web sites. Thus, the focus in many situations could be on achieving ways of cooperatively sharing domain names, rather than on deciding who has a “better” right to a particular Internet domain name.

B. “Classic” Cybersquatting

“Classic” cybersquatting, as contemplated here, is the practice of registering one or more domain names with the intention of

---

*microsoft.com* and simply type the domain name into the URL bar of the Web browser without using a search engine at all. However, less well-known trademarks and domain names may be used in this way to the disadvantage of the trademark holder.


s selling them for a profit to someone who has a particular interest in the domain name, most obviously the holder of a registered trademark corresponding to the domain name. As noted above, one of the earliest and most prominent examples of this involved the activities of Dennis Toeppen, who registered over one hundred domain names corresponding to well-known trademarks.116 In the early days of electronic commerce, Toeppen foresaw how valuable these domain names could become before many of the big corporations recognized their potential.117 He sought payment from the relevant corporations for transfer of the domain names to them.118 Toeppen was subsequently sued by a number of corporations on trademark infringement grounds for transfer of the relevant domain names to the “rightful” holders.119

One of the better known cases against Toeppen was the litigation involving the panavision.com domain name, in which Panavision International brought proceedings against Toeppen under the pre-ACPA domestic trademark law.120 This case was of particular interest, in that it was unclear at the time precisely how, or whether, traditional trademark law would, or should, deal with such cybersquatting activities. Ultimately the court in the Panavision case, as in most other similar litigation, held in favor of the trademark holder.121

This dispute arose when Toeppen asked Panavision to pay him $13,000 in return for a transfer of the panavision.com domain name to them, along with a promise that Toeppen would not acquire any other Internet domain names alleged by Panavision to belong to them.122 Toeppen did not include any content on his panavision.com Web site to suggest that he had any connection with Panavision, nor did he pass off any of the Web site contents as belonging to, or otherwise being authorized by, Panavision.123 In fact, he included only photographs of aerial views of the town of Pana, Illinois.124 After Panavision refused to pay Toeppen the $13,000, Toeppen

---

116. These included domain names corresponding to trademarks owned by Delta Air Lines, Neiman Marcus, Eddie Bauer, Lufthansa, American Standard, and U.S. Steel. Panavision II, 141 F.3d 1316, 1319 (9th Cir. 1998).
118. Id.
119. Id.
120. Panavision II, 141 F.3d at 1319.
121. Id. at 1327 (holding that Toeppen's actions were aimed at Panavision with an intent to extort and, thus, were a clear violation of the Federal Trademark Dilution Act, 15 U.S.C. § 1725(c) (2000), and the California antidilution statute).
122. Id. at 1319.
124. Id.
registered a domain name corresponding to another Panavision trademark, *panaflex.com*. The only content on the relevant Web page was the word "Hello."

The Ninth Circuit Court of Appeals had little trouble in holding that Toeppen had committed a trademark infringement by diluting Panavision's trademarks. Judge Thompson noted that, in his view, a domain name is more than just an "address." It has the significant purpose of identifying the entity that owns the relevant Web site. In response to Toeppen's argument that his conduct did not prevent Panavision from registering some other domain name and using its registered trademarks within the relevant Web site, the court noted that using a company's trademark as its domain name is the easiest way to locate a company's Web site. Relying on a search engine could turn up hundreds of Web sites, and the plaintiff's Web site would not necessarily be prioritized in the search results. The court was concerned that Panavision could lose customers if people were forced to wade through multiple Web sites produced by search engines rather than being able to type the intuitive *panavision.com* into their Web browser to take them directly to the Panavision Web site. As noted above, the court also seemed concerned with the immorality of Toeppen's conduct generally and found that the attempt to sell the relevant domain names to Panavision was a "commercial use," for the purposes of the Lanham Act.

Presumably, if the Toeppen situation arose today, under the UDRP, Toeppen would be ordered to transfer the relevant domain names to Panavision and, indeed, to other corporations in a similar position, on the basis that: (a) his domain names were identical or confusingly similar to trademarks held by other entities; (b) he had

125. *Panavision II*, 141 F.3d at 1319.
126. *Id.*
127. *Id.* at 1327. "Dilution" is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of—(1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake or deception." 15 U.S.C. § 1127 (2003). The Trademark Dilution Act provides a cause of action for a party injured by dilution. *Id.* § 1125(c).
128. *Panavision II*, 141 F.3d at 1327.
129. *Id.*
130. *Id.* at 1326-27.
131. *Id.* at 1327. In today's marketplace, search engines can turn up thousands or millions of Web sites in search results as compared with the potential "hundreds" of search results referred to in the *Panavision* judgment.
132. *Id.*
133. *Id.* at 1325-26. See also Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1239 (N.D. Ill. 1996) (making similar observations that Toeppen's cybersquatting conduct amounted to a "commercial use" of the relevant mark for the purposes of trademark law).
no rights or legitimate interests with respect to the domain names; and (c) he registered and used the domain names in bad faith.\textsuperscript{134} Under the provisions of the ACPA, a similar result would likely be achieved. In addition to the above rationale, a court applying the ACPA would be encouraged to take into account, as bad-faith factors, Toeppen's pattern of registering multiple domain names that he knew were identical or confusingly similar to the trademarks of others,\textsuperscript{135} and the fact that he offered to sell the domain names to relevant trademark owners for a profit.\textsuperscript{136} The application of these rules is hardly surprising given that both the UDRP and the ACPA were drafted specifically to combat conduct such as Toeppen's.\textsuperscript{137}

What is interesting about the way in which these laws and policies have developed in the wake of early domain name/trademark cases is the fact that those early cases clearly set the stage for the presumption that trademark protection would be a paramount concern in cyberspace. Despite the very real concerns of the plaintiffs in \textit{Panavision} and other similar cases, the question remains whether trademark law was the appropriate vehicle for dealing with the plaintiffs' problems. As noted above, Toeppen was not using the plaintiff's trademarks in \textit{Panavision} in a traditional manner of infringement, and he makes quite compelling arguments that his activities did not prevent the plaintiff from using their marks online, nor did they confuse customers as to the source of goods or services.\textsuperscript{138} Additionally, not all jurisdictions subscribe to the "infringement by way of trademark dilution" doctrine that is prevalent in the United States.\textsuperscript{139} Thus, the result in the \textit{Panavision} litigation may have been difficult to replicate under domestic trademark laws in some other jurisdictions. This is where the UDRP has come in handy for trademark holders on a more global scale.

The legacy of cases like \textit{Panavision} was that the subsequent development of the domain name system proceeded with trademark

\textsuperscript{134} See UDRP, supra note 3, § 4(a).
\textsuperscript{136} \textit{Id.} § 1125(d)(1)(B)(i)(VI).
\textsuperscript{138} \textit{Panavision II}, 141 F.3d at 1324-27.
concerns at the forefront, and the remedies for domain name disputes were developed on the basis of trademark considerations. This may be too narrow a view of the domain name system for the twenty-first century, as the following case studies demonstrate. Obviously, the existence of the UDRP and the ACPA does not necessarily prevent other policies and regulations from developing with respect to domain names where a trademark interest is not the only concern in a particular dispute. However, the presumption has now arguably been created that trademarks are of paramount importance in the domain name regulation area, particularly in the “.com” space. Thus, other interests created in the future—for instance, in personal names or cultural identifiers—are likely to be subservient to trademark considerations.140

The Internet is an unparalleled communications medium in terms of speed and scope. The domain name system was not originally developed with electronic commerce in mind, although the rise of electronic commerce has been unprecedented and the medium is clearly very well suited to such transactions.141 However, it is not clear that the global information society has truly asked, or answered, questions as to how we want the domain name system to operate and how we want to prioritize the allocation of domain names. Obviously, in the early days of the system, the idea behind the domain name registration system was “first come, first served.”142 There was clearly no preconception that corporate entities with valuable trademarks would have “better” rights in domain names, at least until the litigation started to occur. Thus, there is a possibility that trademark holders have, to some extent, “hijacked” the domain name system through reliance on trademark rights to powerfully influence the development of domain name policy and to encourage the evolution of legal and regulatory mechanisms skewed toward protection of trademarks.

This is not to say that such developments are necessarily illegitimate or wrong but, rather, that they occurred without sufficient thought as to the nature and future of the domain name system. In particular, the question was not asked whether domain names should be allowed to influence the development of trademark policy, or vice versa. In some ways, this parallels the way in which the copyright system was incrementally altered by judicial decisions, leading to pressure for amendments to copyright legislation, in order to meet the needs of software producers and other digital content

140. Second WIPO Report, supra note 102, ¶¶ 199-201.
141. First WIPO Report, supra note 137, ¶ 10.
142. E.g., New Generic Top-Level Domains, supra note 5, ¶ 13.
industries. These legal developments were in response to very real needs of corporate entities. However, in developing relevant laws and policies, insufficient time may have been taken in order to examine closely the extent to which copyright policy should be influenced by new forms of information technology.

The following discussion questions the suitability of the ACPA/UDRP approach for various kinds of disputes. It suggests that, while the ACPA and the UDRP may be well suited to traditional bad-faith cybersquatting activities, a broader approach to domain name disputes needs to be developed for other classes of disputes. In particular, it is important to recognize that many domain name disputes are not about protecting a registered trademark holder against a bad-faith cybersquatter.

C. "Noncommercial" Cybersquatting

A set of domain name disputes that is particularly problematic under the current system incorporates activities that may be described as cybersquatting because they involve the registration of a domain name that corresponds with someone else's trademark. However, in this class of cases there is no clear or overriding intent to make a commercial profit directly from attempting to sell the name to the relevant trademark holder. There are many and varied reasons why a person would engage in such conduct. For instance, she may want to register a domain name corresponding to someone else's trademark to make comments about the entity with the registered mark, such as to criticize or parody that entity's activities. Examples of these kinds of motivations are evident in the cases of Planned Parenthood Federation of America v. Bucci,144 People for the Ethical Treatment of Animals, Inc. v. Doughney,145 and, more recently, Bosley Medical Institute v. Kremer.146

1. Planned Parenthood Federation of America v. Bucci

Planned Parenthood Federation of America v. Bucci involved a Web site registrant using a domain name derived from another entity's registered service mark, "Planned Parenthood," in an attempt to present messages critical of the plaintiff's activities and point of view.147 The plaintiff was a nonprofit organization that

145. 263 F.3d 359, 363 (4th Cir. 2001).
146. 403 F.3d 672, 674-75 (9th Cir. 2005).
provided "resources regarding sexual and reproductive health, contraception and family planning, pregnancy, sexually transmitted diseases, and abortion." At the time of the litigation, it was operating its Web site under the domain name ppfa.org. The defendant, host of a Catholic radio program, was very critical of the stance the plaintiff took on abortion and contraception. He registered the plannedparenthood.com domain name in order to attract Internet users who might be pro-abortion or otherwise think they were accessing the plaintiff's Web site. The domain name was then used in an attempt to provide anti-abortion and related information to those people.

This is obviously not a clear cut case of using a domain name corresponding to someone else's trademark to directly criticize the trademark holder or her activities. The defendant's conduct here was a little more oblique, in that it had the potential to confuse Internet users looking for the plaintiff's Web site as to the source of the information on www.plannedparenthood.com. Furthermore, the defendant did other things to facilitate confusion, such as including the text "Welcome to the PLANNED PARENTHOOD HOME PAGE!" prominently on the Web site. Thus, the defendant apparently attempted to pass off his views on abortion as those of the Planned Parenthood Federation of America, and he used the domain name to attract Internet users potentially sympathetic to Planned Parenthood's activities in order to provide information contradictory to the organization's views.

In terms of cybersquatting, this was also not a case of a bad-faith registration of a domain name to extort money from the "rightful" owner of the mark, unlike the Toeppen-style, "classic" cybersquatting scenarios. Here, the defendant did not want to sell the domain name to the Planned Parenthood organization. He wanted to use the domain name himself for his own commentary on various social issues.

Ultimately, he was held liable for trademark infringement under the pre-ACPA laws of the United States. This case raises a number of similar concerns to those raised in the above discussion of the Panavision case. In particular, it was not clear that the defendant's activities were truly infringing the plaintiff's interests

148. Id. at 1432.
149. Id.
150. Id.
151. Id. at 1433.
152. Id.
153. Id. at 1432.
154. Id. at 1433.
155. Id. at 1437, 1441.
in a traditional trademark-dilution sense. The court went to some lengths to find the requisite commercial uses of the trademarks by the plaintiff and defendant to support trademark infringement proceedings under the pre-ACPA Lanham Act. Unlike the Panavision litigation, however, the court could not base commercial use on the defendant's attempt to sell the domain name to the plaintiff because the defendant had no such intention. However, the court found that the commercial use requirement was satisfied for a number of reasons, including the fact that any activities on a Web page are likely to be "in commerce" because audiences of any Web page that are widely dispersed geographically will be using national or international telephone lines to access relevant material. Additionally, the defendant was interfering with the plaintiff's ability to provide services in forty-eight states and over the Internet, which, according to the court, must satisfy the "in commerce" requirements of the Lanham Act.

Again, as with Panavision, if this litigation were decided under the ACPA, it would, presumably, be a clear case of infringement. Under the ACPA, when applying the bad-faith factors, the court would likely have taken into account the defendant's intent to divert consumers from the [service] mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark... with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the [Web] site.

This case is, perhaps, another good example of a hard case making bad law and ultimately leading to bad remedial legislation. Like Panavision, it is questionable whether trademark law was the right paradigm to apply here, even if one accepts that the defendant's conduct was facially immoral. The increasing use of trademark law in these types of scenarios might skew both the development of domain name policy and the traditionally accepted policy basis of trademark law. Nevertheless, the reason for mentioning Planned Parenthood here is to show that cybersquatting

156. Id. at 1434-37.
157. Id. at 1433.
158. Id. at 1434.
159. Id.
161. Compared to the Panavision situation, the defendant here was at least arguably trying to provide a social service to the community, by promulgating an alternative point of view to the plaintiff's information, although he went about it in a morally questionable manner. See Planned Parenthood, 42 U.S.P.Q.2d at 1433.
can occur for purposes other than an intention to profit from selling the domain name to a person with a corresponding registered trademark interest. The ACPA groups these situations together under the bad-faith factors. However, it may be more effective to tease out the different kinds of motivations for cybersquatting and to treat them differently if they are not all truly about commercial profit. If we are going to protect more interests online than commercial trademark interests, a more sophisticated approach to domain name disputes should be developed.

Consider, for example, a case in which someone wanted to register a domain name like plannedparenthood.com and make it clear that they were not endorsed by the Planned Parenthood Federation of America, but were using the site to criticize Planned Parenthood's ideas and activities. In the Planned Parenthood litigation, the court assumed that, even if the defendant had included a disclaimer on his Web site making it clear that his Web site was not endorsed by the plaintiff, there would still have been a trademark infringement. This finding was made on a basis similar to the argument accepted in Panavision that a domain name is more than a mark; it is a home page address that serves as an external label to direct Internet users to a Web site. The court suggested that it would be trademark infringement to register a domain name corresponding to another person's trademark and to criticize that person's activities, even with a disclaimer making it clear that there was no endorsement to do so.

However, it is not clear that this argument is necessarily borne out. The validity of this conclusion depends on whether we view the social function of the domain name system as being predominantly a means of facilitating commercial trademark interests or whether we wish to promote other interests that may include criticism or parody of the activities of a given trademark holder. Even if the aim is to promote online commerce, it is not clear that cases like Planned Parenthood are really about protecting online commerce, at least in the context of traditional trademark policy.

2. People for the Ethical Treatment of Animals v. Doughney

Other situations have arisen involving activities that may be classed as cybersquatting in the technical sense, but where the purpose is not to sell the relevant domain name to a corresponding trademark holder for commercial profit. In People for the Ethical Treatment of Animals, Inc. v. Doughney, the defendant registered

---

162. Id. at 1441.
163. Id.
164. Id. at 1439-40.
the domain name peta.org, which corresponded to the plaintiff's commonly used acronym and service mark, PETA. The defendant used the domain name to create a Web site called "People Eating Tasty Animals." In his defense, he claimed that the Web site was a parody of the plaintiff's organization and activities. He did not pass off his site as being endorsed by the plaintiff, and the Web site "contained links to various meat, fur, leather, hunting, animal research, and other organizations." The defendant did not offer to sell the domain name to the plaintiff, although, when asked by the plaintiff to transfer the name, he refused and later commented that, if PETA wanted one of his domain names, they should make him an offer. The defendant was ultimately found liable for service-mark infringement and for violating the ACPA, and the domain name was transferred to the plaintiff. He was unsuccessful in arguing that he did not intend to make a financial profit from registering the domain name, as is necessary in a defense under the ACPA, because he had publicly commented that PETA could make him an offer for the domain name if they wanted it. Further, the court held that several of the ACPA's bad-faith factors clearly covered the situation at hand. The court particularly noted that the defendant had no legitimate interests in the mark and that he was purposely using the mark to confuse people who might be searching for the plaintiff's Web site. The court also took into account that the defendant had registered other names in the past that corresponded to trademarks and people's names and engaged in similar conduct; in terms of setting up parody Web sites.

Again, we might ask whether trademark law is really the appropriate vehicle for these kinds of disputes or whether it is actually quite a poor fit in these kinds of cases. No one would likely argue that the defendant's conduct was particularly pleasant or responsible. However, if we regard the Internet as an unparalleled global communications medium, rather than a purely commercial forum, should we not have better, more appropriately tailored rules to deal with these kinds of situations? In this case, PETA was arguably not really concerned with trademark infringement but,

165. 263 F.3d 359, 362-63 (4th Cir. 2001).
166. Id. at 362.
167. Id. at 363.
168. Id.
169. Id.
170. Id. at 363-64, 367-69, 371.
171. Id. at 368.
172. Id. at 368-69.
173. Id. at 369.
174. Id.
rather, with the message the defendant was advocating and the use of a domain name that could be intuitively associated with the organization. PETA was not really worried about its ability to use its trademark or service mark in commerce, nor was it concerned that the defendant was confusing consumers in the sense of appropriating its potential customers. Relying on trademark legislation and the UDRP might ultimately damage the policy paradigm underlying trademark law and may create results, with respect to domain name disputes, that do not accord with developing social values and expectations, in terms of the domain name system.

3. Bosley Medical Institute, Inc. v. Kremer

In fact, the skewing of trademark policy seemed to be a matter of concern to the Ninth Circuit Court of Appeals in the more recent case of Bosley Medical Institute v. Kremer. This case raised a factual situation somewhat similar to that in PETA, but the Ninth Circuit took a different view to that taken by the Fourth Circuit in PETA. Bosley involved a patient of the Bosley Medical Institute setting up a “gripe site” to criticize the Institute’s hair restoration services. The defendant Kremer registered the domain name bosleymedical.com for his Web site, despite the plaintiff’s registration of the “Bosley Medical” trademark. The plaintiff brought proceedings against Kremer under traditional trademark law, as well as under the ACPA. The basic trademark infringement actions failed at both the district court level and on appeal to the Ninth Circuit on the basis that the use of the plaintiff’s trademark in Kremer’s domain name was “noncommercial” in the trademark sense and was unlikely to cause any consumer confusion. However, the Ninth Circuit reversed the district court’s summary judgment on the ACPA claim on the basis that the district court erred in applying a “commercial use” requirement to the ACPA claim as well as to the trademark infringement claims.

In its analysis of the trademark infringement claims, the Ninth Circuit rejected the PETA approach due to the fact that it would place most critical consumer commentary of a plaintiff’s activities under the regulation of the Lanham Act. In its conclusions on the

175. 403 F.3d 672, 674 (9th Cir. 2005).
176. Id. at 675.
177. Id. Kremer also registered www.bosleymedicalviolations.com, which was not challenged by the plaintiff. Id.
178. Id. at 674.
179. Id.
180. Id. at 674, 679-80.
181. Id. at 681.
182. Id. at 679.
basic trademark infringement claims, the *Bosley* court noted that:

Kremer is not Bosley's competitor; he is their critic. His use of the Bosley mark is not in connection with a sale of goods or services—it is in connection with the expression of his opinion *about* Bosley's goods and services.

The dangers that the Lanham Act was designed to address are simply not at issue in this case. The Lanham Act . . . does not prohibit all unauthorized uses of a trademark . . . . Any harm to Bosley arises not from a competitor's sale of a similar product under Bosley's mark, but from Kremer's criticism of their services. Bosley cannot use the Lanham Act either as a shield from Kremer's criticism or as a sword to shut Kremer up.183

These judicial comments evidence clear concern that some recent cases have been going too far in their broad interpretation of trademark laws in an attempt to protect trademarks against all forms of undesirable corresponding domain name registrations, even when the protection of traditional trademark interests is not necessarily at stake.184 Thus, the *Bosley* decision is obviously a step in the right direction, with respect to concerns about blurring the boundaries of traditional trademark law. However, that question may now be moot, in light of the enactment of the ACPA and the adoption by ICANN of the UDRP. Even the *Bosley* court left the question of ACPA infringement open, noting that a successful ACPA action does not necessarily require the satisfaction of a "commercial use" requirement, and that it remains to be seen whether Bosley could have established that Kremer registered the relevant domain name in bad faith.185 We can now only anticipate whether such conduct might fall afoul of the ACPA without necessarily infringing more traditional trademark rules. If this is the case, the question as to whether the ACPA adds anything to traditional Lanham Act liability for cybersquatting may finally be answered in the affirmative.186 Whether bad faith should be found in such cases as a matter of policy is a more complex question.

183. *Id.* at 679-80.
184. *Id.* See also Hannibal Travis, *The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet*, 10 VA. J.L. & TECH. 1 (2005), at http://www.vjolt.net/vol10/issue1/v10i1_a3-Travis.pdf (suggesting that courts have found corresponding domain names to violate trademark law, even when traditional trademark principles are not involved).
185. *Bosley*, 403 F.3d at 681.
186. This is assuming, of course, that the Ninth Circuit decision is correct on the trademark infringement issue.
The *Bosley* litigation certainly raises some interesting questions about the kinds of social values we might want to protect in a domain name registration and dispute resolution system. “Gripe sites,” like that set up by the defendant in *Bosley*, raise specific questions about the role of the domain name system and domain name policy with respect to the balance between commercial rights and interests and free speech interests. Certainly, there is a social value in allowing people to have easy access to a forum to complain about the activities of a commercial entity. However, the question remains whether these people should be able to utilize a domain name for that forum that somehow corresponds with a trademark associated with the relevant entity.

On the one hand, the use of such a domain name is a certain way of reaching a large audience with a message critical of the business in question. If the person who wishes to complain about a business is relegated to a “lesser” domain space, she might be unable to attract the kind of audience that she wants to reach. On the other hand, is there a social value in the expectation that a “.com” name, in particular, that corresponds to a trademark will lead to a Web site affiliated with the trademark owner? Further, there may be situations in which a relevant trademark owner does not want to maintain a Web site or a Web presence. Should that trademark owner then be forced to register one or more domain names defensively and to maintain registration, in order to prevent potential gripe sites from arising under a relevant domain name? This Article suggests that it should not always be the case that a trademark owner has the “best” rights in a corresponding domain name, but that conclusion still leaves unresolved difficult questions as to where appropriate lines are to be drawn.

4. airfrancesucks.com

These questions become even more difficult when one considers slight variations of the facts in *Bosley*. A recent WIPO arbitration dealing with the domain name *airfrancesucks.com* is a good case in point. The domain name here is not *airfrance.com*. In other words, it is not a direct transcription to domain name form of a valuable trademark. However, it clearly incorporates the “Air France” trademark in a prominent manner. This case involved a complaint and commentary Web site on which visitors to the site

---

187. See discussion infra pp. 143-49.
were encouraged to register complaints about experiences they had in flying with Air France. The WIPO arbitration panel was split as to whether the domain name should be transferred to the complainant, Air France. The majority panelists ultimately ordered transfer of the name to Air France on the bases that the domain name was confusingly similar to the “Air France” trademark, the registrant had no legitimate rights in the name, and the registrant had registered the domain name in bad faith. However, a dissenting panelist felt that domain names utilizing a trademark plus a pejorative word like “sucks” would not confuse consumers about the source of information on the Web site.

Perhaps a discussion of this case does not really belong in the “noncommercial” cybersquatting category of disputes, as defined above in Parts IV.A and IV.C, because it is arguably not a cybersquatting dispute like the ones litigated in the previous cases, which involved domain names that directly corresponded to a trademark without any additional pejorative words. It may be that the addition of a pejorative term like “sucks” at the end of a domain name could answer the “social values” question raised within Part IV.C.3. Perhaps the best balance of social interests would be achieved by allowing gripe site operators to utilize a “sucks” version of a name and preventing them from using a domain name that identically corresponds with a relevant mark. Under this scenario, a gripe site could be operated under airfrancesucks.com, but not under airfrance.com. However, this does not deal with the problem that the ability to use an identically corresponding domain name like airfrance.com or bosleymedical.com will probably attract a larger audience than relegating people who wish to complain about a business to a gripe-site suffix like “sucks.” It also does not deal with the problem of uses of domain name suffixes that are not clearly pejorative. What would have happened, for example, if the respondent in the Air France case had utilized a domain name like www.airfrancetickets.com for its gripe site?

There is certainly much more work to be done in the gripe-site context in terms of examining previous disputes involving such sites and the various permutations and combinations of domain names that are utilized in this context, as well as the closeness of their association with a given trademark. This Article does not aim to definitively resolve the gripe-site question other than identifying that both the policies behind trademark law—to avoid consumer

189. *Id.* § 5(B).
190. *Id.* §§ 6-7, Dissent (Samuel, Arb., dissenting).
191. *Id.* §§ 6-7.
192. *Id.* at Dissent (Samuel, Arb., dissenting).
confusion and, to some extent, to avoid dilution of famous marks—and the importance of promoting free speech are competing social values that should be protected in cyberspace. The question is, particularly in relation to gTLDs like “.com,” what should the overriding policy choices be with respect to uses of domain names corresponding to trademarks that are not operated by direct commercial competitors to the trademark holder? It is important that the international Internet community starts to consider these questions in more detail and to separate the various permutations and combinations of motivations for cybersquatting conduct outside of the “classic,” direct commercial profit motives.

5. mcdonalds.com

Moving away from the gripe-site context, one final example of a cybersquatting case that did not involve a pure commercial profit motive may well be of historical interest only, but it exemplifies further how unexpected motivations may lead to the registration of a domain name that corresponds with someone else’s trademark. In the early days of the Internet, a journalist from Wired magazine, Joshua Quittner, realized that domain name registration was like the western frontier, and that domain name prospectors, like Toeppen, were snapping up domain names that large corporations might later want to possess. He noticed the lack of awareness by large corporations of the Internet and the domain name system, as well as the lack of careful scrutiny of registration applications by the domain name registry in the early days of domain name registration. Specifically, he spoke to the McDonald’s Corporation and asked a representative about the company’s awareness of the Internet and domain name registration issues, noting that mcdonalds.com was not yet registered and also suggesting that anyone could register it, including the McDonald’s Corporation’s chief competitor at the time, the Burger King Corporation.

Ultimately, Quittner registered mcdonalds.com himself to make this point. He set up an e-mail address of ronald@mcdonalds.com and solicited suggestions from people for what to do with the domain name. Ultimately, he agreed to transfer the domain name to McDonald’s in exchange for them making a contribution to

194. Id.
195. Id.
196. Id. at 56.
197. Id.; Bitlaw, supra note 103.
Again, this is an example of an activity that we would today categorize as cybersquatting. Presumably, under the UDRP and the ACPA, this kind of conduct would fall afoul of the respective bad-faith factors, because Quittner had no legitimate interest in the domain name and did not use it for any legitimate purposes, unless one considers raising public and corporate awareness of the potential for trademark-infringing uses of Internet domain names a legitimate purpose.\(^1^9^9\)

It is true that Quittner did not intend to make a profit for himself from registering the name, but he ultimately achieved a commercial gain for a charity, so this conduct may still violate the ACPA. The ACPA only requires that the defendant "has a bad-faith intent to profit from that mark," and it does not define what "profit" means in this context.\(^2^0^0\) Given the fairly broad interpretations that courts have generally made regarding trademark law,\(^2^0^1\) and the ACPA in particular, conduct such as Quittner's, carried out in today's marketplace, might be blocked by this obstacle. In terms of the bad-faith factors, Quittner, or someone engaging in conduct such as his in today's market, might face problems due to the fact that they would have no legitimate interests in the mark and they would be usurping a domain name that "rightfully" belonged to someone else. It would, arguably, be similar to the position in which Doughney found himself during the PETA litigation.\(^2^0^2\)

It is possible, however, that Quittner, engaging in similar conduct today, could defend himself against a bad-faith finding under the UDRP on the basis that: (a) he did not register the domain name "primarily for the purpose of selling" it to McDonald's for a profit;\(^2^0^3\) (b) he did not engage in a pattern of registering domain names corresponding to well-known trademarks;\(^2^0^4\) (c) he did not register the domain name "primarily for the purpose of disrupting the business" of McDonald's;\(^2^0^5\) and (d) he did not attempt to attract customers to his Web site by passing it off as being sponsored or endorsed by McDonald's.\(^2^0^6\)

\(^{198}\) Bitlaw, supra note 103.

\(^{199}\) See supra Part III.A-B.


\(^{201}\) See supra notes 138-43 and accompanying text.

\(^{202}\) People for the Ethical Treatment of Animals, Inc. v. Doughney, 263 F.3d 359, 369 (4th Cir. 2001).

\(^{203}\) UDRP, supra note 3, § 4(b)(i).

\(^{204}\) See id. § 4(b)(ii).

\(^{205}\) Id. § 4(b)(iii). This proposition is perhaps questionable, although, at the time, the McDonald's Corporation apparently had no plans for an Internet presence, so, in that context, it might have been difficult to argue a purpose of "disrupting the business." Id.

\(^{206}\) See id. § 4(b)(iv).
This is a somewhat frivolous example because it is perhaps unrealistic in this context to look at conduct that occurred in the early days of the Internet when few people truly understood its potential as a commercial medium, including the potential of domain names to be valuable online commodities. On the other hand, pre-ACPA and -UDRP situations may give us an idea of how people originally perceived the domain name system, prior to the rise of regulatory mechanisms that favored commercial trademark interests. In any event, the Quittner situation is mentioned here because it does highlight the fact that there may be unpredictable reasons for which someone would want to register a domain name corresponding to an unrelated, valuable trademark without an intent to profit personally from, or to infringe upon, the trademark.

Thus, trademark law may have its limitations as a regulator of online conduct involving domain name registration and use. In the future, it is likely that the global Internet community will need to look at these issues more closely. It may be that anticybersquatting legislation and private dispute resolution mechanisms ultimately will need to be reviewed in order to answer questions relating to the potential impact of these systems on competing social interests. These interests might include the ability of individuals to utilize relevant domain names for purposes such as the criticism or parody of a trademark holder.

At the very least, the “noncommercial” forms of cybersquatting should be separated, as a matter of policy, from “classic,” Toeppen-style cybersquatting in making these determinations. “Classic” cybersquatting is clearly an easier case because no obvious social or cultural interests are served by permitting this kind of activity, and there is an arguably obvious “bad-faith” or profit motive. Most of the scenarios classified above as “noncommercial” cybersquatting, however, potentially raise competing social interests to those of the trademark holder, usually in the free speech area. Thus, the ability to promote some of these interests should be addressed more precisely than is currently the case under existing dispute resolution mechanisms.

It may be that the solution to this problem is to make better use of differentiated gTLDs in this context. Perhaps there needs to be a rule that the “.com” suffix should be reserved for trademark interests, and that a new suffix should be introduced for use of commentary and parody Web sites. The problem with this solution is that it assumes that the possession of a trademark gives an entity an automatic right to one or more corresponding “.com” level

---

207. See supra Part IV.B.
208. See supra Part IV.C.
versions of its trademark, and it also assumes that those wishing to comment on the entity holding that trademark should be relegated to a "lesser" domain space. There has apparently been no conscious regulatory decision that this rule should be implemented, and there is no necessary policy reason why it should. Further, it is not clear that trademark law is the appropriate vehicle to achieve this result, even if it is accepted that commercial trademark interests should take priority in the "com" name space. Indeed, the court in Bosley expressed its opinion that trademark law is not intended to prevent all unauthorized uses of a trademark, even if such uses do occur within a corresponding domain name.\footnote{Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 679 (9th Cir. 2005).}

Further, the reason that people like Kremer register "com" level domain names for gripe sites is to draw attention to their criticisms of the relevant commercial entity. If Kremer had been relegated to a lesser form of the "Bosley" domain space, he would not have achieved his desired purpose of publicly criticizing Bosley's practices in a significantly large online forum. Again, the question arises as to whether trademark law and policy is the appropriate vehicle for regulating such conduct. In any event, the PETA case involved a "org" domain name.\footnote{People for the Ethical Treatment of Animals, Inc. v. Doughney, 263 F.3d 359, 362 (4th Cir. 2001).} Thus, even a rule that "com" names should be reserved to "rightful" trademark owners would not solve the problem of commentary and parody sites utilizing other important gTLDs such as "org" and "net." If there is to be a presumption that all gTLDs corresponding to trademarks are to be reserved for "rightful" trademark owners, whether or not those trademark owners have bothered registering the names before someone else, this edict should be the result of clear, and preferably global, policy debate.\footnote{In fact, this has been the case with respect to some of the newer gTLDs introduced in 2000. Policy decisions were made to allow legitimate trademark holders and, in the case of the "name" and "pro" domain spaces, other legitimate interest holders to have priority in registering relevant domain names to avoid cybersquatting. The strategies for doing so are comprehensively discussed and evaluated by WIPO in its report, \textit{New Generic Top-Level Domains}. \textit{See supra} note 5, ¶¶ 95-107. However, these policies were never implemented for the original gTLDs such as "com," "org," and "net."}
D. Contests between Multiple Legitimate Interests

Moving away from cases involving activity that might be described as cybersquatting, another category of disputes in which trademark principles might not provide the answers for determining a contest between competing interests in a domain name is the situation where two or more parties have competing "legitimate" interests in the domain name. The obvious contest here is between two or more parties who each hold trademark interests that correspond to the same domain name. This is different from what has been termed "cybersquatting" in the previous two categories, largely because the key aim of the registrant here is not to claim a particular domain name in the absence of a commercial trademark interest therein with the knowledge that another entity has such an interest corresponding to the name. Rather, the registrant itself has a commercial trademark interest in the name, regardless of whether she knows that another party may also have a competing trademark interest in the name.

This can occur, for example, when the same or a similar mark has been registered in the same jurisdiction, but with respect to different goods or services.\(^{212}\) Another example would be where a similar mark has been registered with respect to similar goods or services but in different jurisdictions.\(^{213}\) The problem here arises from the fact that domain names are unique, whereas multiple similar trademarks may be registered at different trademark registries, or at the same registry, but regarding different goods and services. Thus, disputes over domain names can arise that national trademark systems are ill-equipped to handle.

1. delta.com

Obviously, it is possible for different versions of a similar domain name to be registered: for example, microsoft.com, ms.com, microsoftcomputing.com, microsoft.net, and microsoft.org. However, as noted above, most businesses will want to register the domain name that most obviously, generically, and intuitively leads people to their Web site. Thus, businesses will prefer a ".com" level domain name with wording that most clearly identifies their business. Delta Air Lines, for example, will want to ensure that it can register

---

\(^{212}\) Similar trademarks can be registered for different goods and services within one jurisdiction and even for similar goods and services in different jurisdictions because of the national character of trademark registration systems.

\(^{213}\) This occurred with ConAgra's "Healthy Choice" trademark, which was registered in Australia independently of ConAgra's American operations. See ConAgra Inc. v. McCain Foods (1992) 33 F.C.R. 302.
delta.com, as well as the more convoluted deltaairlines.com.\textsuperscript{214} This example also highlights the associated point that one trademark holder can register more than one domain name.\textsuperscript{215} As mentioned previously, the online retailer Amazon.com has registered various country-code level versions of its domain name, along with amazon.com and amazon.biz.\textsuperscript{216} The idea of releasing multiple new gTLDs was partly that various legitimate interest holders could all have at least one version of a relevant domain name. However, it does not appear to have worked out this way in practice. The “.com” domain names are still the most highly coveted, and nothing stops businesses with a legitimate interest in a domain name from registering multiple versions of the name, as the Delta Air Lines and Amazon.com examples illustrate.\textsuperscript{217}

The delta.com name is actually a very good example of a set of competing legitimate interests in the same “.com” domain name corresponding to multiple registered trademarks. In recent years, much litigation has been threatened and settlements ultimately reached, with respect to the delta.com name.\textsuperscript{218} There were a number of companies who wanted the name, each of whom managed to register it for a particular period of time.\textsuperscript{219} This included Delta Air Lines, Delta Financial, and DeltaComm Internet Services,\textsuperscript{220} each of which would appear to have a legitimate right to use the name. The domain name was, in fact originally registered to DeltaComm, who then sold it to Delta Financial when it could not reach a satisfactory transfer agreement with Delta Air Lines.\textsuperscript{221} Ultimately, Delta Air Lines obtained the domain name from Delta Financial.\textsuperscript{222}

This is a classic situation in which trademark law and current

\begin{itemize}
  \item[215.] \textit{See New Generic Top-Level Domains}, supra note 5, \textsection 21.
  \item[216.] \textit{See supra} note 20 and accompanying text.
  \item[217.] \textit{See New Generic Top-Level Domains}, supra note 5, \textsection 21 (suggesting that a large number of trademark owners are likely to register their marks in all possible gTLDs).
  \item[219.] \textit{Id}.
  \item[220.] \textit{Id}.
  \item[221.] \textit{Id}.
  \item[222.] \textit{Id}.
\end{itemize}
domain name dispute resolution policies do not provide the answers to some significant commercial problems. All of the trademarks were validly registered, and all of the companies involved in the domain name dispute had a legitimate claim to the name. Each of the companies, in fact, could have used a different gTLD version of the domain name, such as delta.org or delta.biz, but the "com" name was perceived to be more valuable. Additionally, they could all have used longer and more descriptive versions of the "com" name, such as deltaairlines.com, deltacomm.com, and deltafinancial.com. In this vein, the Delta Faucet Company uses deltafaucet.com.

2. roadrunner.com

Another example of a situation in which two or more entities might have had a legitimate claim to the same domain name involved the roadrunner.com domain name. This was a pre-ACPA and -UDRP case, but it is illustrative of the point being made here. The name roadrunner.com was originally registered to an Internet access provider in New Mexico. Many companies in New Mexico


226. At the time of writing, Delta Financial is using the deltafinancial.com domain name. See http://deltafinancial.com (last visited Nov. 22, 2005).


228. See Bitlaw, supra note 103.
are named after the Roadrunner bird because it is the state bird of New Mexico, and any number of them could plausibly assert rights to the roadrunner.com domain name. Warner Bros. Entertainment Group disputed the registration of the domain name by a New Mexico company on the basis of the name's relationship with its popular "Road Runner" cartoon character. Network Solutions, Inc., the company responsible for registration of "com" domain names at the time, threatened to suspend the registration of this domain name on the basis of complaints from Warner Bros., so the New Mexico company sued Network Solutions to prevent the suspension. Although suspension was prevented, the domain name was eventually obtained by a joint venture company involving Time Warner, MediaOne, Microsoft, Compaq, and Advance/Newhouse.

Again, we see a poor fit between standard trademark law principles and the Internet domain name system. Even as augmented by the UDRP and the ACPA, this dispute would have been difficult to resolve, as the competing interests all appeared to be legitimate. Thus, it would have been hard to establish any bad-faith factors to justify an order to transfer the name to the complainant Warner Bros. This may simply mean that a "first-come, first-served" rule should apply to such disputes and that market forces will sort out who has the better interest in a domain name, in terms of who is prepared to pay the most for a transfer of the name. However, such an approach will likely favor rich and powerful corporations over smaller businesses, which have fewer resources either to fend off litigation or to pay high market prices for desired domain names.

There may be nothing wrong with this result as a matter of policy. In fact, there may be social value in allowing the wealthiest corporate entity to hold the most intuitive version of a particular domain name. If it is assumed that, among competing parties, the corporation with the greater resources to secure the domain name

230. Oppedahl, supra note 1, at 441.
232. Bitlaw, supra note 103.
233. Id.
also has a larger online customer base, then, perhaps, this result makes sense, because a larger group of customers is less inconvenienced in searching for the entity in question. However, once again, this possibility has never been consciously debated as a matter of global Internet policy.

Furthermore, there may also be distinct social value in promoting the activities of less wealthy entities online because of the potential of the Internet to enable such entities to develop in a more expansive way than they could manage in the purely physical world. While large corporate entities may have an advantage in the physical world, promoting smaller entities' interests online may create business opportunities that would not otherwise exist for these entities and thereby serve values relating to the diversification of business activity and consumer choice online. In fact, one way to assist both larger and smaller online entities and to promote both sets of social values online would be domain name sharing arrangements. Under such arrangements, one or more entities could share, for instance, the ".com" version of the same domain name on a shared Web page, which would, in turn, contain hyperlinks to the different entities' respective Web sites.

3. clue.com

One final example of a dispute involving multiple legitimate interests in a single domain name involves the clue.com name. This domain name was, during the course of the dispute, and is still, at the time of writing, registered to Clue Computing, Inc. Clue Computing is an information technology consulting company that chose its corporate name without reference to the popular "CLUE" board game that is manufactured by Hasbro, Inc. Hasbro has registered the "CLUE" trademark with respect to the game. In litigation between Hasbro and Clue Computing, the founder of Clue Computing noted that he and his partner had chosen the name for their business in response to people referring to themselves as being "clueless" about computers. Thus, the founders of Clue Computing thought it would be clever to have a business whose name played on the idea of giving clueless people a "clue." As a result, much

litigation has ensued between Hasbro and Clue.\footnote{239. For a summary of this litigation, see Clue Computing, Inc., Hasbro, Inc. sues Clue Computing, Inc., at http://www.clue.com/legal/index.html (last modified May 28, 2002).}

To date, Hasbro has been unsuccessful in having the domain name transferred to it on the basis of trademark infringement.\footnote{240. See supra note 235 and accompanying text.} Hasbro has not been able to demonstrate, under the Lanham Act, that Clue Computing is either diluting its trademark or causing any significant consumer confusion.\footnote{241. Hasbro, 66 F. Supp. 2d at 124-26.} Even under the ACPA or the UDRP, it is unlikely that Hasbro could establish the requisite bad-faith factors against Clue Computing, as Clue Computing does appear to have a legitimate claim to the domain name. As noted above, Hasbro, as the larger corporation, could always offer to pay Clue Computing a significant amount for the domain name. However, as the last significant action relating to this litigation took place in the year 2000,\footnote{242. Hasbro, Inc. v. Clue Computing, Inc., 232 F.3d 1 (1st Cir. 2000).} it would seem that Hasbro may have lost interest in the domain name.

This may be an example demonstrating that the market eventually sorts itself out with respect to many commercial conflicts involving domain names with multiple potentially legitimate commercial uses. It may also go some way towards alleviating the concerns raised above with respect to the \texttt{roadrunner.com} name and, to some extent, the \texttt{delta.com} name, that large corporations will always win out in a market system because they can force the smaller corporations into submission through costly litigation and eventually out-pricing them for the desired domain name. However, this may not be the best example to quell concerns about the domination of larger commercial players in these kinds of conflicts. Presumably, Hasbro does not have as significant an interest in the \texttt{clue.com} domain name as Delta Air Lines has in \texttt{delta.com}, because of the direct association of the domain name with Delta's corporate identity.

Hasbro may even have a lesser interest in the \texttt{clue.com} name than Warner Bros. has in the \texttt{roadrunner.com} domain name. Although "Clue" is the name of a product distributed by Hasbro, and "Road Runner" is the name of a cartoon character developed by Warner Bros., there is likely a stronger association between Warner Bros. cartoon characters and the Warner Bros. corporate identity than between board games and their manufacturers. The only evidence that somewhat supports this proposition is the way in which Warner Bros. arguably pursued the \texttt{roadrunner.com} domain name more aggressively than Hasbro pursued \texttt{clue.com}. However,
Warner Bros.' ultimate success and Hasbro's ultimate failure might, instead, be a result of the fight that was put up by the respective smaller corporations that possessed a competing interest in the relevant domain names. Clue Computing may have taken a more strident stance than the New Mexico Internet access provider, both as a matter of principle and, perhaps, because they received more financial and other support from outsiders.\footnote{Clue Computing made a specific call for financial support on their Web site. See Clue Computing, supra note 239.}

This may support an argument that, in cases of legitimate competing commercial interests in a domain name, the market will sort itself out with little help necessary from any external legal or regulatory system. Sometimes, the bigger corporation will win, and, sometimes, it will lose. Regardless of the outcome, it is clear that traditional trademark law and policy, as it is now augmented by the UDRP and the ACPA, is not a good fit for these kinds of disputes. It is also clear that little thought has been given to alternate methods for dealing with these disputes outside of the policies based on traditional trademark law as altered by the new laws. Certainly, there have been no detailed national or global debates about the kinds of social and commercial values that should be promoted in these situations as a matter of policy.

4. Domain Name Sharing

Perhaps these kinds of disputes lend themselves to new approaches. One potential solution would include entities with competing legitimate interests in a domain name sharing that name by a joint registration and then sharing a home page with hyperlinks to individual Web sites of the respective interest holders. Technically, this possibility is not particularly problematic. Thus, if a government policy (or private ICANN policy) could be developed to encourage this kind of activity as an alternative to litigation or dispute resolution, society might benefit through greater accessibility to all Web sites, with similar trademark identities utilizing a mutual domain name as a portal to their respective Web sites.

One way of encouraging this kind of activity would be for a government agency or private body authorized by ICANN to specialize in helping those prepared to share a domain name with the technical aspects of setting up the shared main Web page with hyperlinks to the respective entities' individual Web sites. This could be a free service funded, in part, by domain name registration fees, or it could be a service offered inexpensively by the relevant
agency or department as an alternative to more costly litigation or dispute resolution.\footnote{244} This approach might necessitate some revision to the UDRP, as well as to the initial domain name registration licensing agreement, in order to make it clear that the "first-come, first-served" rule will not necessarily apply in a case of multiple competing legitimate trademark interests corresponding to a domain name. Under the scheme proposed here, domain name registration policy might have to reflect the fact that, in cases of competing legitimate interests, domain name sharing is to be mandated over permitting the first registrant to maintain the name, in the absence of a showing of a bad-faith registration under the UDRP or the ACPA by a complainant. Otherwise, there would be no incentive for an initial domain name registrant to participate in a domain name sharing scheme, assuming that the registrant felt that she could successfully deflect a UDRP complaint or an ACPA action on the basis of her rightful ownership interest in a trademark corresponding to the relevant domain name. Such a scheme would also likely require, for applicants seeking a domain name sharing arrangement, a showing of a good-faith interest corresponding to the relevant domain name.

There are a number of ways to set up this kind of a system. As suggested above, domain name sharing could be incorporated into the UDRP. Thus, if the initial registrant objected to sharing the relevant domain name under a private arrangement, an arbitrator or panel of arbitrators might determine whether to mandate a domain name sharing arrangement. Such arbitration would, presumably, be instituted by the nonregistered party wishing to share the name.

This is not as difficult as it might at first appear. During the course of standard UDRP complaints, arbitrators already routinely determine whether domain name registrants and complainants have legitimate interests in a disputed domain name.\footnote{245} It should not be too imposing to ask those arbitrators to make similar determinations in a different context. In other words, a new part of the UDRP could be developed in order to empower arbitrators to order a domain name sharing arrangement in the event that a complainant shows a legitimate interest in a domain name in which the original domain name registrant also has a legitimate interest. Such a system might also allow for a complainant to argue, in the alternative, both for a transfer of the domain name, if the original

\footnote{244. Thus, any fee charged for this service should be less than the cost of a UDRP dispute resolution proceeding.}
\footnote{245. See UDRP, supra note 3, § 4(a)-(c).}
registrant is found not to have a legitimate interest in the name, and, failing that, for a domain name sharing order, in the event that the registrant is found to have a legitimate interest. Ultimately, the sharing system could be extended to multiple shared registrations, provided that all claimants could establish a legitimate interest in utilizing the domain name.

E. Personal Names

Another area in which trademark policies, including those developed to address cybersquatting, are proving to be a poor fit for regulating domain name disputes is in the area of personal names. Sometimes, personal names operate like trademarks, particularly when attached to celebrities who may hold some trademark, or trademark-like, rights in their names due to the commercial goodwill attached to the names. However, personal names may have various social values attached to them. Not all celebrity names operate as trademarks. Personal names of celebrities and noncelebrities alike may further contain elements worthy of legal protection on alternative bases, such as privacy policy. Additionally, personal names may be used publicly for other important social reasons outside of the purely commercial arena. An obvious example is political purposes. It is likely that trademark principles and privacy policies are both poor fits for the protection of politician names. Some new principles might need to be developed to regulate registration of domain names corresponding to politician names.

The following discussion considers issues that may arise during the course of registration of domain names that correspond to: (a) a celebrity's name; (b) a politician's name; and (c) a private individual's name, when that person is neither a celebrity nor a politician. This discussion illustrates the fact that the domain name system's current reliance on principles of trademark and unfair competition law and policy has left important policy gaps in the regulation of domain name registration. This discussion further suggests that it may now be necessary to reconsider what kinds of legal rights should inhere in private individuals with respect to the registration of domain names that correspond to their personal names.

246. This argument would be made under the existing UDRP provisions. See id. § 4(i).
247. See infra Part IV.E.1.
249. See infra Part IV.E.1.
250. See infra Part IV.E.2.
251. See infra Part IV.E.3.
names, particularly in the ".com" space.\textsuperscript{252}

The discussion also emphasizes the fact that this area of domain name policy has increasing international significance because of the global reach of the Internet and the fact that multiple persons around the globe may share a similar, or identical, name. Contests may arise as to who has superior rights to domain names that correspond to personal names when different people share those names and when each of them has very different interests in the corresponding domain names. Additionally, disputes may arise, particularly in the celebrity and political arena, as to who has better rights to a domain name that corresponds with a celebrity or politician personal name and that may be used to host a Web site that comments favorably or unfavorably on the activities of the person in question. Finally, there is a question as to whether an individual's right to a domain name corresponding to her personal name should be limited to an affirmative right to use the name herself, or whether it should be extended to a right to prevent or restrict others from using the relevant domain name, even if she has no desire to use the name herself.

1. Celebrity Names

Celebrity names have already fueled some disputes under the UDRP. High-profile disputes will often arise involving the names of famous actors and musicians. One well-publicized dispute involved a domain name corresponding to the name of Julia Roberts, the Academy Award-winning actress who has appeared in a number of well-known films, including \textit{Pretty Woman},\textsuperscript{253} \textit{Notting Hill},\textsuperscript{254} and \textit{Erin Brockovich}.\textsuperscript{255} On November 9, 1998, Russell Boyd registered the domain name juliaroberts.com.\textsuperscript{256} Boyd placed a photograph of a woman named Sari Locker on the Web site, and he later placed the domain name up for auction on the commercial auction Web site, \textit{www.eBay.com}.\textsuperscript{257} At the time, Boyd had registered over fifty other domain names, including domain names which incorporated the names of other famous movie actors such as Madeleine Stowe and Al Pacino.\textsuperscript{258}

\begin{itemize}
\item \textsuperscript{252} A recent WIPO report considered some of these issues with respect to the newer, and less well utilized, "name" space. \textit{New Generic Top-Level Domains}, supra note 5, ¶¶ 95-107.
\item \textsuperscript{253} \textit{PRETTY WOMAN} (Touchstone Pictures 1990).
\item \textsuperscript{254} \textit{NOTTING HILL} (Universal Pictures 1999).
\item \textsuperscript{255} \textit{ERIN BROCKOVICH} (Universal Pictures 2000).
\item \textsuperscript{257} \textit{Id}.
\item \textsuperscript{258} \textit{Id}.
\end{itemize}
In March 2000, Julia Roberts commenced a UDRP arbitration proceeding against Boyd from which she successfully obtained an order that the domain name be transferred to her.259 As of the date of this writing, the domain name is not in use.260 The basis for the decision in the arbitration was that Julia Roberts had a common law trademark right in her name and, further, that Boyd had no legitimate rights or interests in the name and registered and used the domain name in bad faith.261

This decision may seem unremarkable in its results on policy grounds. Presumably, many of us would agree that a famous actress has a legitimate interest in ensuring that a domain name corresponding to her personal name is not used in a manner unauthorized and potentially damaging, either personally or professionally. She may or may not have been particularly concerned with Boyd's actual use of the domain name at the time of the arbitration proceeding. Her concern may have primarily been with what might happen if someone bought the domain name on eBay and used it in a harmful way. On the other hand, she may have been concerned that Internet users would type juliaroberts.com into an Internet browser and be taken to a Web site that had nothing to do with her. This latter possibility seems unlikely as Roberts herself has not, in the ensuing years, used the domain name for any kind of authorized fan Web site.

The real question stemming from this dispute regards the nature of the actual legal and policy basis for the decision. For Roberts to have succeeded under the terms of the UDRP, she was forced to establish common law trademark rights in her personal name because this is the basis for claiming a right in a domain name under the UDRP.262 It may not always be easy for celebrities to


262. UDRP, supra note 3, § 4(a)(i).
establish this kind of interest in a domain name corresponding in whole, or in part, to their personal names. Additionally, it may well be impossible for noncelebrities to establish common law trademark rights in their names for the purposes of UDRP policy. Additionally, the Roberts case is a relatively easy case because Boyd had no apparent legitimate competing interest in the domain name. The UDRP might not be as helpful in situations where the validity of the domain name’s alternative use is not so clear cut. Boyd, for example, has retained his registration of the \textit{alpacino.com} domain name but has inserted an unofficial fan site on the corresponding Web page presumably to avoid losing another domain name challenge.

UDRP arbitrators have certainly had to walk a fine line in terms of determining whether a competing use of a celebrity name in a domain name is a legitimate use. In a case involving the domain name \textit{brucespringsteen.com}, a WIPO administrative panel was forced to decide whether an unofficial fan site could use the name in the face of a challenge by famous singer Bruce Springsteen himself. The domain name had been registered in 1996 by Jeff Burgar in Canada, who used the name for an unauthorized fan Web site. Like Boyd in the \textit{Roberts} arbitration, Burgar had registered multiple domain names corresponding to the personal names of famous people. The arbitration panel, however, ultimately held that Burgar was making a legitimate, noncommercial use of the domain name and that Springsteen had failed to show that the domain name was registered or used in bad faith. This decision was not unanimous, though, with one dissenting panelist arguing that the domain name should be transferred to Springsteen.

In comparing the \textit{Roberts} and \textit{Springsteen} arbitrations, several trends in domain name regulation come to light. These trends were perhaps already apparent in the drafting of the UDRP, but the \textit{Roberts} and \textit{Springsteen} arbitrations bring these issues into sharp relief. First, it is clear that the domain name system, as currently regulated, relies heavily, perhaps overly so, on the establishment of trademark rights, or trademark-like interests, in domain names, even when the domain names correspond to personal names. It may

\begin{itemize}
\item 263. \textit{See infra} Part IV.E.3.
\item 265. \textit{Id.} § 5.
\item 266. \textit{Id.}.
\item 267. \textit{Id.} §§ 6, 7.
\item 268. \textit{Id.} \textit{at} Dissent (Page, Arb., dissenting).
\end{itemize}
be possible for famous actors and singers to establish such rights, but it will be difficult for many other people to demonstrate these kinds of interests in their personal names. Even some well-known celebrities may have trouble establishing requisite trademark-like rights in their personal names. The same is likely true of many politicians. The majority panel in the Springsteen arbitration was not fully convinced that Springsteen could support a claim for trademark rights corresponding to his personal name. The majority was, however, prepared to assume that he did have such rights, as the arbitration could be decided on other grounds:

It is common ground that there is no registered trademark in the name “Bruce Springsteen.” In most jurisdictions where trade marks are filed, it would be impossible to obtain a registration of a name of that nature. Accordingly, Mr. Springsteen must rely on common law rights to satisfy this element of the three part test [under the UDRP].

It appears to be an established principle from cases such as Jeanette Winterson, Julia Roberts, and Sade that in the case of very well known celebrities, their names can acquire a distinctive secondary meaning giving rise to rights equating to unregistered trade marks, notwithstanding the non-registrability of the name itself. It should be noted that no evidence has been given of the name “Bruce Springsteen” having acquired a secondary meaning, [or] in other words, a recognition that the name should be associated with activities beyond the primary activities of Mr. Springsteen as a composer, performer and recorder of popular music.

In the view of this Panel, it is by no means clear from the UDRP that it was intended to protect proper names of this nature. As it is possible to decide the case on other grounds, however, the Panel will proceed on the assumption that the name Bruce Springsteen is protected under the policy . . . .


270. See infra Part IV.E.2.


272. Id.
Given this attitude by the majority panelists in the *Springsteen* decision, it is possible that many celebrities, even very well-known celebrities, could have a difficult time establishing the requisite trademark interests in their personal names for UDRP purposes. This would certainly suggest that noncelebrities would likely be unable to establish such rights at all and, accordingly, that the UDRP would not protect any interests in domain names corresponding to personal names of noncelebrities. The *Springsteen* majority panel noted that it was unconvinced that the UDRP is intended to protect proper names. However, this leaves open the question of whether we need any kind of legal policies or rules that would protect such names, either as an addendum to, or independently of, the UDRP. In the United States, the ACPA has, to some extent, filled this gap. However, the ACPA's approach to protecting personal names is arguably out of step with much of traditional trademark policy and has not been followed on the global stage. Additionally, it has some serious practical limitations, in that it requires the bad-faith registrant to have a profit motive by seeking to sell the domain name either to the person with whose name it corresponds or to a third person. In practice, this is not always the case when personal names are involved in domain name disputes, although it was the case in the *Roberts* dispute.

A second point to note arising from the *Roberts* arbitration and, especially, the *Springsteen* arbitration is that, even where trademark interests in a name can be established by a complainant, a respondent does not have to go to very much effort to set up some form of legitimate competing interest in a disputed domain name. Presumably, Boyd established his unauthorized Al Pacino fan site in the wake of the *Roberts* decision to ensure that he did not lose the *alpacino.com* domain name. The site is not particularly sophisticated, nor is it by any means comprehensive. It is likely that it is being used to prevent a successful challenge by Al Pacino or his management. It would seem, from the *Springsteen* arbitration, that any kind of commentary on a Web site relating to a celebrity, no matter how superficial, will suffice to show a legitimate competing interest in the relevant domain name. Thus, it will be

273. *Id.*
274. *See infra* notes 77-78 and accompanying text.
very difficult for a celebrity, or anyone else, for that matter, to prove that any vaguely justifiable use of a domain name is not a legitimate, good-faith use of the name for UDRP purposes.

Thus, the UDRP generally provides only weak protection for personal names, including the personal names of celebrities, which are the most likely candidates for protection under the UDRP, as celebrities are the group of people most likely able to establish some form of trademark rights in their personal names. This result raises a number of questions about the regulation of domain names corresponding to personal names. Should anyone have a legally protected right in a domain name corresponding to their personal name? If so, should celebrities have different rights than noncelebrities, either on the basis of commercial goodwill associated with their personal names or on some other basis? If there are legal rights in domain names corresponding to personal names, should they be in the nature of affirmative rights to use the name in commerce, as desired by Bruce Springsteen, or should they also encompass negative rights to prevent the name from being used at all by anyone, as apparently desired by Julia Roberts?

For the most part, these questions pertain to various different classes of personal names that correspond to domain names, not simply to celebrity names. However, it is interesting to begin discussion about them in the celebrity-name context. For example, does Julia Roberts really want to assert a commercial property-like right in juliaroberts.com, like Bruce Springsteen apparently did with his corresponding domain name, or, rather, does she want the protection of a privacy-like right? If her aim is to prevent anyone from using the domain name, it may be that this is an area for development of some privacy law principles.

The problem with drawing such a distinction between different possible legal bases for such rights in domain names would ultimately relate to the costs and difficulties inherent in establishing precisely why a particular celebrity sought transfer of a given domain name. Julia Roberts may, in reality, have a number of reasons for seeking the domain name in question—perhaps both to protect her privacy in controlling unauthorized content being disseminated on a www.juliaroberts.com Web site and also partly to preserve her later ability to commercialize the domain name herself.


280. Once again, at the time of this writing, Roberts has not done so. Currently, the domain name is registered to Allen Klayman. Network Solutions, WHOIS Record for juliaroberts.com, at http://www.networksolutions.com/whois/results.jhtml?jsessionid=I52OIFXWCCOI4CWKEAPSFFA?whoistoke
The question also arises as to whether it is efficient for people to veto the use of particular domain names when it is possible that someone else, other than the original, bad-faith registrant, may have a legitimate use for the name. What if a private individual named “Julia Roberts” also wanted the name for a personal Web site and was barred from utilizing it because the celebrity Julia Roberts acquired the name with no desire to use it herself? Should the noncelebrity be relegated to the “.name” suffix, for instance, as a matter of domain name policy? These are questions that cannot be answered by traditional commercial trademark policy. They require more detailed consideration of developing global norms relating to Internet use and perceptions of the domain name system outside the electronic commerce context.

Should ICANN, WIPO, or some other organization, for example, be maintaining a register of nonpermitted uses of specific domain names that would, nevertheless, allow registration and use for other purposes? This might be similar to a restrictive covenant system on a land title registry. Should the celebrity Julia Roberts be entitled to veto registration of the juliaroberts.com domain name for particular purposes, without: (a) being required to maintain registration of the name herself; and (b) thereby preventing others from making use of the name in a manner non-objectionable to her?

If we were to develop such a “veto” system, what would be the legal basis of Roberts’ rights in the domain name: property, privacy, or something else? If it works like a land title registry with restrictive covenant-like notations, then it sounds like a property interest, even though Roberts may only be intending to guard her privacy. This suggestion raises some difficult questions of legal theory which may or may not need resolution before such a system could be practically implemented. It may be that the nature of the precise legal rights at issue here defies classification under traditional legal categories and that a new form of domain name rights corresponding to personal names must be developed for these purposes.

In fact, this suggestion is not unlike some of the strategies adopted with respect to the registration of some of the newer gTLDs since 2000. In a recent report, the WIPO Arbitration and Mediation

---

281. For more general discussions about how land law principles relating to rights and obligations of land use could be incorporated into the cyberlaw/information law area, see Michael A. Carrier, Cabining Intellectual Property through a Property Paradigm, 54 DUKE L.J 1 (2004); Jacqueline Lipton, Information Property: Rights and Responsibilities, 56 FLA. L. REV. 135 (2004).
Center evaluated some of the "preventive" measures\textsuperscript{282} taken in the new gTLD spaces, such as ".name" and ".pro," in order to restrict undesirable uses of domain names in these spaces\textsuperscript{283} Some of the strategies employed in these newer domain name spaces included: (a) setting up a "watch" service to enable people with a legitimate interest in a mark, word, or name corresponding to a domain name to be notified if anyone attempted to register the name, without a requirement that the "watcher" register the name herself;\textsuperscript{284} and (b) a "defensive registration" service that allows a person with a legitimate interest in a domain name to register it without having to actively use it.\textsuperscript{285} The report also discusses the viability of "exclusion mechanisms" that would prevent the registration of domain names by people likely to utilize them in undesirable ways.\textsuperscript{286} However, such exclusion mechanisms have not yet been implemented with respect to any of the new or old gTLDs.\textsuperscript{287}

The "veto" system suggested above is, perhaps, a little more sophisticated than these alternative approaches, because it focuses on allowing the use of a given domain name for specific purposes and only vetoing its use for undesirable purposes. It does not potentially take a particular domain name off the market altogether if someone wants to register it defensively or object to its registration by someone else. However, this veto system does have the disadvantage of requiring the development of policy guidelines as to the basis and scope of potential impermissible uses of a given domain name. This is likely to be a complex task and one in which bodies like WIPO and ICANN may be loathe to engage. Further, if such a scheme were ever to be implemented, it might require administrative oversight with more complex determinations than are required by domain name "watch" services, "defensive registration" services, or even basic "exclusion mechanisms." The administrative oversight required for a veto system may, thus, be much more costly and time consuming than these alternatives.

In fact, a de facto "veto" scheme may actually be achievable

\textsuperscript{282} In the report, "preventive" measures are contrasted with "curative" measures. Preventive measures refer to measures that can be taken prior to a dispute arising in order to minimize the possibility that a dispute will arise by allowing an interested person some measure of control over a domain name corresponding to a legitimate interest in the domain name. Curative measures relate to dispute resolution procedures that are utilized after a dispute arises. New Generic Top-Level Domains, supra note 5, ¶ 22. Preventive and curative measures can be utilized in concert, as the following discussion will demonstrate.

\textsuperscript{283} Id. ¶¶ 95-107.
\textsuperscript{284} See id. ¶¶ 120-21.
\textsuperscript{285} See id. ¶ 122.
\textsuperscript{286} See id. ¶ 123.
\textsuperscript{287} Id.
under the current domain name registration system without the need to create a registry of impermissible uses of particular Internet domain names. Assuming that an individual like Julia Roberts would be able to gain control of a relevant domain name utilizing the UDRP procedures, she could then make private arrangements to transfer or license that name to a new user for an agreed upon, legitimate purpose. However, there are three main weaknesses with this solution, as compared with developing a more formalized registry system as contemplated above.

First, as noted above, it is not always easy, under current domain name policy, for affected individuals to gain control of domain names corresponding to their own personal names, particularly in the "".com," "net," and "".org"" domain spaces. The ability to do so would have to be built into a new system to make any of these solutions workable. Second, having gained control of such a name, the ""rightful registrant"" would need to have some incentive to allow legitimate, non-objectionable uses to be made of the name by another person. It is not immediately obvious what such incentives might be, assuming that the registrant would have the option of simply holding the name and preventing all unauthorized uses of it. Finally, even if the registrant did permit a non-objectionable use of the name by private contract, reliance on such agreements has the obvious drawback that they are only enforceable between the contracting parties. Thus, if a transferee or licensee of a relevant domain name later sold or licensed it to a third party for impermissible purposes, the original registrant would potentially be limited in her legal recourse, aside from returning to the UDRP and starting again with a new arbitration proceeding against the third party. These risks may well mitigate against people entering into private arrangements to facilitate legitimate, unobjectionable uses of particular domain names.

On the other hand, perhaps private individuals and celebrities, in particular, should have no specific legal rights in relation to "".com," "".net,"" or "".org"" domain names corresponding to their personal names, outside of any trademark interests that may have become associated with the name. If the true concern is with Web site content, perhaps such individuals should always be required to structure their complaints in terms of, for instance, defamation law, privacy law, or the ""celebrity tort"" in relevant jurisdictions.

288. A good example of the use of privacy-like laws to protect celebrity interests was the use of the breach of confidence and the breach of relevant provisions of the European Union Data Protection Directive in the litigation brought by Catherine Zeta-Jones and Michael Douglas against a freelance journalist and a variety of publications that published unauthorized photographs of their wedding. See Douglas v. Hello!, [2003] 3 All E.R. 996 (Q.B.
Domain name registration is, arguably, one step removed from actual Web site content and should be treated accordingly by the legal and regulatory system. Domain names could be regarded as merely one of many possible indicators as to where an Internet user may find particular information about a given celebrity. On this analysis, the complainant should focus on Web site content, rather than who has registered a particular domain name.

In this vein, the respondent in the Springsteen arbitration made an analogy between Internet domain names and magazine covers. He suggested that the mere use of the name of a celebrity on the front page of a magazine does not mean that the magazine is claiming any kind of specific rights in relation to the name, but merely that it features content about the individual in question. This argument contemplates the use of a domain name as a pointer to published information about a celebrity, whether the information is authorized or unauthorized and independently of whether the publisher of the information might be subject to any liability with respect to the content of the information. This might suggest that the UDRP should not protect any celebrities' interests in "*.com," "*.net," or "*.org" names corresponding to their personal names and, perhaps, that the law should focus on the content of Web sites and not the control of a particular domain name in these cases.

However, the main problem with this suggestion is that it implicitly assumes that these categories of domain names should only be legally protected in the hands of their "rightful" owners, when they connote a traditional trademark interest and not when they protect other socially important interests, like identities of individuals, whether or not the individuals are trying to control permitted uses of their names in a trademark sense. Again, it assumes a limited role for domain name policy outside the protection of commercial trademark concerns, and, even then, the current policy only protects those concerns in the face of bad-faith cybersquatters and not against those making legitimate, if Ch. 2003). See also, e.g., A v. B p.l.c., [2003] 3 W.L.R. 542 (C.A. 2002); Wainwright v. Home Office, [2002] 3 W.L.R. 405 (C.A. 2001); Douglas v. Hello!, [2001] 2 W.L.R. 992 (C.A. 2000); Greitje Baars, Grasping at Nettles: An Analysis of the Douglas v. Hello! Case, 3 PRIVACY & DATA PROTECTION 7 (2003).


291. Id.
superficial, uses of the name, at least in the celebrity-name context. If this decision has, in fact, been made at a policy level, it has been made too rashly and too early in the development of Internet usage to take into account other important emerging social norms in relation to domain name usage. It is more likely that such a policy decision has never been consciously made by any government or regulatory authority. Rather, commercial trademark cybersquatting was the most pressing concern in the 1990s, and it is the main issue that has been expressly dealt with to date as a matter of policy, particularly in the "com," and, to some extent, also the "net" and "org" domain spaces. It is now time to start regulating other aspects of domain name policy.

As noted above, Congress has created a special protection for domain names corresponding to personal names under section 1129 of the Lanham Act (as part of ACPA revisions to the Act). This pre-dated the introduction of the "name" space and was drafted with the original gTLDs, such as "com," "net," and "org," in mind. To succeed under this section, the complainant must establish that the defendant had an intent to profit from selling the domain name. This is consistent with the aim of the ACPA to prevent traditional cybersquatting activities. However, the profit motive may not always be evident in situations where individuals are seeking to prevent certain uses of domain names corresponding to their own personal names. Although Julia Roberts could have utilized this approach with respect to Boyd's attempt to sell juliaroberts.com on eBay, people like Bruce Springsteen and Al Pacino could not have availed themselves of section 1129 against the individuals who simply maintained unauthorized fan sites attached to the relevant domain names brucespringsteen.com and alpacino.com. There was no apparent attempt to sell either of those names to the "rightful" owners, nor to anyone else as required by section 1129.

The section 1129 approach also appears unlikely to be adopted on a more global scale. The Report of the Second WIPO Internet Domain Name Process rejected a call to insert similar considerations into the UDRP, feeling that this would make UDRP disputes more confusing and difficult to decide, in that it would raise a complex set of privacy and property rights in relation to certain domain names. WIPO was concerned that the incorporation of

292. One example of the latter is the current alpacino.com Web site. See supra note 258 and accompanying text.
293. See supra note 79 and accompanying text.
294. See supra note 72 and accompanying text.
295. See supra Part III.C.
296. Second WIPO Report, supra note 102, ¶¶ 199-203.
such a provision in the UDRP might "jeopardize the credibility and efficiency of the UDRP," particularly given the lack of international norms about protecting rights in personal names. 297 This may well have been a legitimate concern in 2001, when the UDRP was fairly new and needed to be developed, accepted, and understood by the Internet community.

However, now that the UDRP is well established and is relatively successful within its limited sphere of operation, it might be time to start developing new international policies relating to the protection of rights in personal names that could be implemented alongside the current UDRP provisions. This would allow a more comprehensive, if more complex, system of domain name dispute resolution procedures to develop, in order to better account for the complex relationships that can arise in relation to domain names. Such a system could involve elements of domain name sharing, as suggested above, as well as the possibility of establishing a register of impermissible uses of particular domain names that could be requested by those with a particular personal, or perhaps even cultural or religious, 298 interest in a given domain name. Such a register could draw from strategies employed in relation to the "name" space, such as the "watch" service and "defensive registration" service described above. 299

2. Politician Names

Politician names raise several more complex issues than do celebrity names in the domain name context. While at least some celebrity names will be protected under the provisions of the UDRP, it appears relatively clear that politician names will not be protected by the policy unless the politician in question can establish a commercial value in the name, in the commercial trademark sense. 300 As noted above, the UDRP requires a showing of a trademark, or trademark-like interest, in a personal name that corresponds to a domain name, in order for an arbitration proceeding to be successful. 301 There is some evidence that politician names will not likely fit the bill here.

One of the landmark decisions under the UDRP involved Kathleen Kennedy Townsend, who, at the time of the complaint, was a second-term lieutenant governor of the State of Maryland and a potential 2002 gubernatorial candidate. 302 Ultimately, her bid for

297. Id. ¶ 201.
298. See discussion infra Part IV.F.
299. See supra notes 284-85 and accompanying text.
300. See supra notes 47, 50, 53 and accompanying text.
301. See supra notes 261-62 and accompanying text.
that office was unsuccessful.\footnote{Jabeen Bhatti & S.A. Miller, *Ehrlich Wins in Stunning Upset: First Republican to Take Maryland Since Agnew in ’66, WASH. TIMES*, Nov. 6, 2002, at A1.} Prior to the election year, the respondent in the proceedings had registered a number of domain names corresponding to Townsend’s name, allegedly for the purposes of selling them to her for a profit.\footnote{Townsend, Case No. D2002-0030, § 4.} Although this was the kind of dispute for which section 1129 was inserted into the Lanham Act, Townsend proceeded under the UDRP and lost her claim on the basis that the WIPO arbitration panel did not feel that she, as a politician, could establish a sufficient trademark interest in her personal name on which to succeed in a UDRP proceeding.\footnote{Id. §§ 6-7.}

The panel did, however, note that it is possible that a political organization might have sufficient trademark rights in a candidate’s name or slogan upon which to base a UDRP challenge to a domain name registration.\footnote{See Townsend, Case No. D2002-0451, (WIPO Arb. and Mediation Ctr., Admin. Panel Decision, July 31, 2002) (Plant, Davis III, Page, Arbs.), at http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0451.html.} It further noted that, in the United States, at least, the ACPA might provide some relief for politicians in Townsend’s position.\footnote{Id. § 6. Note that a later proceeding brought by a political group on behalf of Townsend, Friends of Kathleen Kennedy Townsend, also did not result in a transfer of the domain name. See Friends of Kathleen Kennedy Townsend v. Birt, Case No. D2002-0451 (WIPO Arb. and Mediation Ctr., Admin. Panel Decision, July 31, 2002) (Plant, Davis III, Page, Arbs.), at http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0451.html.} The panel concluded, however, that the UDRP does not protect politicians against unauthorized registrations of domain names corresponding to their personal names.\footnote{See Townsend, Case No. D2002-0030, § 6; See id. § 7; UDRP, supra note 3, § 4(a).} In particular, the panel referred to the WIPO recommendations mentioned above that clarified the fact that persons who have not profited from a reputation in commerce, as distinct from politics, cannot avail themselves of the UDRP to protect their personal names against parasitic registrations.\footnote{See Townsend, Case No. D2002-0030, § 6; See Second WIPO Report, supra note 102, ¶¶ 199, 202.}

Thus, we see the results of a conscious policy choice at the international level to leave protection of commercially valueless names, at least valueless in the trademark sense, to the vestiges of national laws and norms and not to attempt development of a set of international norms on these issues. This may or may not be a sensible long term strategy, depending on: (a) how global these problems become on the Internet in the future and (b) how effective national solutions prove to be.
It may be that cases of political cybersquatting are peculiarly national in scope. Most politicians are involved in positions on the national, state, or local level. Coupled with WIPO's concerns about the difficulties of formulating international norms on these questions, perhaps this leads to a presumption that these matters are best left to national legal systems for the moment. However, this may well be changing. The European Union, for example, is becoming an increasingly powerful governmental body, the scope of which extends beyond any one set of national borders. Additionally, even among existing nations, the actions of one government often have the ability to impact policies and activities, both social and economic, in other countries. One need only look to the impact that American and British policies have had on the Middle East in recent years to see that it might not only be American norms that should govern the regulation of domain names corresponding to George W. Bush's personal name, nor should it necessarily be only British norms that govern what happens to Tony Blair's name in a domain space.

Of course, one could argue that the above suggestions confuse domain names as Web page identifiers with general free speech rights to comment on government policy. As noted above in relation to celebrity domain names, there is a powerful argument that domain names are merely convenient pointers to Web sites that may contain commentary about a person whose name is reflected in the domain name. Domestic laws will provide liability for commentary that is defamatory, regardless of the pointer that is used to access the commentary. Defamation on the Internet can raise confusing choice of law issues, but this is an issue separate from domain name policy.

In any event, domain name activity with regard to politician

names, again, particularly in the "com" domain space, seems to be increasing and is raising many concerns, both about the regulation of domain name registration and use as well as about the content of Web sites. In the United States, even the ACPA provisions seem to be falling short of meeting some of the perceived needs of players in the political arena. For instance, section 1129(1)(A) of the Lanham Act is targeted at activities that involve an intention to profit from the registration of a person's domain name by selling the domain name either to the person with whose name the domain name corresponds or to a third party. It does not say anything about domain name registrations that are intended to prevent access to a domain name—for example, where a rival political party or interest group wants to hold the domain name "hostage," in order to prevent the "rightful" owner from using it at all.

This will increasingly become a problem in practice, as politicians, in particular, are beginning to realize the potential of the Internet as both a fundraising mechanism and an important communications medium with respect to campaign activity. Both John Kerry and George W. Bush, in the campaign for the 2004 U.S. presidential election, made significant use of their relevant domain names, johnkerry.com and georgewbush.com. The Republican effort had the foresight also to register bushcheney2004.com. However, the Democratic effort was too late to register either kerryedwards2004.com or kerryedwards.com, which were both already registered to others when John Edwards was named as the 2004 Democratic vice presidential candidate.

314. The Lanham Act specifically states that:
Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.
In answer to the question introduced above, there now appears to be a strong argument that the domain name itself is important in a political campaign. If, for example, a Web site is going to be used as a cybercenter for obtaining campaign support, particularly in terms of fundraising, it is important that Internet users can have confidence that a relevant Web site is authorized by the politician or political group in question. As Americans in the lead up to the 2004 presidential election relied on Web sites to access the campaigns, it was important that the Web site purporting to be collecting funds for the Kerry-Edwards presidential bid, for example, was really doing so.

Clearly, if a competing interest group "hijacked" the name and collected funds under false pretenses, this would likely constitute fraud of some description, but it may be very difficult to raise a relevant cause of action and work out precisely who has the standing and resources to litigate. The same would be true of a Web site that looks like it has been authorized by a candidate because of the use of a domain name corresponding to the candidate's name, but that actually contains misinformation about the candidate and his or her policies. The easiest way to regulate this kind of activity is to make sure that the obvious political candidate domain names are registered to the actual candidates, at least for the campaign periods preceding the relevant elections. Here, there is obviously an important social value in preventing political fraud.

Some of the relevant activity is commercial here, particularly as it relates to political fundraising, but it is not commercial in a trademark sense. Thus, it is not appropriately regulated by trademark legislation, even if provisions of a law, such as the ACPA, mistakenly purport to regulate these kinds of activities. There is now some piecemeal state law that attempts to regulate political cybersquatting in terms of the kinds of activities described above. California's recently enacted Political Cyberfraud Abatement Act, for example, creates civil liability for engaging in an act of "political cyberfraud," which is defined in the legislation to mean:

a knowing and willful act concerning a political Web site that is committed with the intent to deny a person access to a political Web site, deny a person the opportunity to register a domain name for a political Web site, or cause a person

---

319. Horn v. Friedman & Co., 776 F.2d 777, 780 (8th Cir. 1985) (noting that the elements of fraud include a false representation of material fact that the defendant knows or believes is false, which the defendant intends the plaintiff to rely on, and that the plaintiff does rely on to his injury).

reasonably to believe that a political Web site has been posted by a person other than the person who posted the Web site, and would cause a reasonable person, after reading the Web site, to believe the site actually represents the views of the proponent or opponent of a ballot measure.\textsuperscript{321}

The definition goes on to give examples of political cyberfraud, including: (a) "intentionally diverting or redirecting access to a political Web site to another person's Web site" by using, inter alia, "a similar domain name,"\textsuperscript{322} (b) "[r]egistering a domain name that is similar to another domain name for a political Web site,"\textsuperscript{323} and (c) "[i]ntentionally preventing the use of a domain name for a political Web site by registering and holding the domain name or by reselling it to another with the intent of preventing its use."\textsuperscript{324} "Political Web site," for the purposes of this legislation, is defined as "a Web site that urges or appears to urge the support or opposition of a ballot measure."\textsuperscript{325}

Although the concerns addressed by the California Political Cyberfraud Abatement Act seem very real, the development of this legislation, in the wake of section 1129(1)(A) of the Lanham Act at the federal level, evidences an increasingly fragmented approach to the issue of cybersquatting involving personal names and political names at the national level. Even within the United States, the relevant laws are becoming fragmented as applied to the regulation of domain names that correspond to personal names. At the international level, this fragmentation is obviously even worse, as alluded to by WIPO in its report rejecting a more expansive scope for the UDRP in this area.\textsuperscript{326}

It may well be the case that the UDRP per se should not be extended to cover nontrademark uses of Internet domain names. However, it is not necessarily true to say that the issue of personal names should not be addressed altogether on a more global level than is currently the case. It is difficult to understand why trademark policy can be regarded as sufficiently globally harmonized to form the basis for a fast, effective, inexpensive, multinational dispute resolution procedure, whereas other uses of domain names have been deemed too problematic for a global approach. Surely, there may be an advantage in formulating general international policy principles regarding domain names that correspond to various classes of personal names, particularly if some

\begin{itemize}
  \item \textsuperscript{321} Id. § 18320(c)(1).
  \item \textsuperscript{322} Id. § 18320(c)(1)(A).
  \item \textsuperscript{323} Id. § 18320(c)(1)(C).
  \item \textsuperscript{324} Id. § 18320(c)(1)(D).
  \item \textsuperscript{325} Id. § 18320(c)(3).
  \item \textsuperscript{326} Second WIPO Report, supra note 102, ¶ 201-02.
\end{itemize}
domain name sharing or temporary compulsory licensing practices could be developed, as suggested in this Article.\textsuperscript{327} Global methodologies should certainly be developed in order to combat political cyberfraud, as well as bad-faith commercial cybersquatting.

In any event, celebrity and political names are not the end of the story here. There is also the issue of personal names without any celebrity or political status, and celebrity names that correspond to other interests that are neither commercial nor political—for example, Madonna.\textsuperscript{328} Further, there is a question of competing interests in other terms that can be used in an Internet domain name, including geographical and cultural identifiers. If we leave domain name regulation predominantly in the hands of trademark law and policy for too long, we may develop a presumption that trademark interests are the most important interests to protect in cyberspace or, worse still, the only thing worthy of protection in cyberspace, at least as far as the domain name system is concerned. We might thus lose the opportunity to create policy principles and regulatory procedures for protecting other important social interests that are potentially impacted by domain name policy.

3. \textit{Names of Private Individuals}

Personal names that do not have any particular celebrity or other public status may also raise interesting questions with respect to domain name regulation. To date, there has not been a significant presumption that a person has any special legal rights in a domain name, aside from in the “.name” space, that happens to correspond to that person’s name, outside of the provisions of the ACPA in the United States. As noted above, the ACPA inserted section 1129 into the Lanham Act in order to create civil liability for a person who registers a domain name that is the same as, or confusingly similar to, a person’s name, without that person’s consent and with the intent to profit by selling the domain to that person or a third party.\textsuperscript{329} There is no corresponding provision at the international level.\textsuperscript{330}

This part of the ACPA appears to have limited practical application to date. This might be because situations have not arisen that involve domain name cybersquatting with respect to personal names that are not sufficiently famous to warrant protection under the UDRP or the more trademark-focused

\textsuperscript{327} See infra Part IV.E.3 (discussing temporary compulsory licensing).

\textsuperscript{328} See infra notes 343-53 and accompanying text.


\textsuperscript{330} See UDRP, supra note 3.
provisions of the ACPA. Private citizens might assume that they have no particular legal rights in their personal names used as domain names, resulting in their choice not to avail themselves of the relevant provisions of the ACPA. On the other hand, it may be that private citizens, in general, simply do not wish to register domain names corresponding to their personal names. Many individuals with their own Web sites will avail themselves of a domain space provided by their employer or Internet service provider. The view may be that, if there is no attempt to draw in customers in a trademark sense, there is no need to have an intuitive domain name. Further, private individuals can now alternatively utilize the "name" domain space for creating a private personal domain name.

Thus, there is a good argument that we do not need to develop any particular laws and policies, other than, perhaps, provisions such as those found in section 1129 of the Lanham Act, in order to protect personal names registered as domain names. This type of provision will protect those who want to register a domain name corresponding to their personal name from predatory domain name cybersquatters. Arguably, little more is needed. If this is the case, there should potentially be no impediment to the adoption of similar provisions at the international level, perhaps as an addition to the UDRP. Such an approach should not be particularly problematic, even taking into account concerns that the UDRP should not become overcomplicated or confusing, leading to a loss of confidence in the arbitration mechanism. A simple provision could be added to the UDRP allowing individuals to bring complaints with respect to registration of a domain name corresponding to the complainant's personal name when the registrant has registered the name in bad faith and has no demonstrable legitimate interest in the name.

Further difficult issues may arise in instances when a domain name corresponding to a personal name also corresponds with a valuable corporate trademark or with a celebrity or politician name. A personal name might even correspond to a cultural reference or geographical place name. It is these contests that will be more difficult. Perhaps the answer here is for a clearer reliance on some of the newer domain name suffixes, such as the "name" space for personal names, and perhaps "org" for some of the cultural

references. Alternatively, the domain name sharing option suggested above, in relation to competing legitimate interests in domain names, might be adopted in these kinds of situations.

There may still be difficulties with other cultural and geographic references that correspond to personal names, and the problem of political names corresponding to private individual's names may also be a concern. The obvious recent example in the United States is the kerryedwards.com domain name, which appears to be jointly registered to two individuals, one of whom has the name Kerry Edwards.\(^{334}\) In such situations, should there be a rule that the political use takes priority in the "com" space during a relevant political campaign and, perhaps, also for any ensuing term of office? It should be noted here that section 1129(1)(A) of the Lanham Act is not particularly helpful in this kind of situation, when both parties—Kerry Edwards and the Kerry/Edwards campaign organization—have legitimate interests in the name.\(^{335}\) In any event, Kerry Edwards, the individual, clearly did not register the name with the intention of extorting money from the Democratic Presidential campaign, as he had registered the name two years before the Kerry/Edwards presidential ticket was announced.\(^{336}\)

In these cases, a temporary compulsory licensing regime could be developed to give rights in a "com" domain space to political domain names during the particular time period for which the name is needed for political purposes. The social value protected here would be the facilitation of communications and fundraising efforts between candidates and the public during an election campaign. An example of how compulsory licensing could be achieved would include an administrative mechanism set up similarly to, or as part of, the UDRP that would encourage private licensing arrangements by mandating compulsory licensing in favor of a bona fide political candidate whose personal name corresponds with the domain name in question. The license could last for the duration of the electoral campaign and might revert back to the original registrant after the campaign. During the license term, the political candidate may be required to pay royalties to the original registrant. Again, this should not be too difficult to achieve in practice, as the only

---

334. The kerryedwards.com domain name was actually registered by Mr. Kerry Edwards in 2002 for $15. In the months preceding the 2004 presidential election, he engaged a professional Internet domain name auctioneer, Sedo.com LLC, to field the six-figure offers he was receiving for the domain name after John Kerry announced John Edwards as his vice presidential running mate. See Press Release, PRWeb, KerryEdwards.com Domain Name to be Auctioned (July 22, 2004), at http://www.prweb.com/releases/2004I7/prweb142903.htm (last visited Nov. 22, 2005).


336. See supra note 334 and accompanying text.
evidentiary requirements would relate to proof of personal names and evidence of candidacy in an election. Licensing fees could be set and updated either by ICANN or by arbitrators in individual cases.

Alternatively, a temporary domain name sharing arrangement might be established along the lines suggested above in relation to legitimate competing commercial interests in a domain name. This might better balance the social value in facilitating political communications with any social values developed in relation to personal domain name use more generally. Again, the process should not be any more administratively complex than a compulsory licensing agreement, as the arbitrators should only have to examine evidence of personal names corresponding to domain names and the existence of an electoral campaign.

There might also be situations in which a political candidate wants to retain a domain name past a temporary licensing period. This could occur either because she won an election or issue and wants to continue to use the name to inform the public of ongoing political developments during an ensuing term of office or because she lost an election or issue but has developed a following of people seeking information from the Web site. In such cases, provision might be made for the compulsory license to continue until one or both parties to the license loses interest in, or use for, the domain name in question. Alternatively, if a particularly long-term license appears to be developing due to ongoing circumstances in which the name is potentially useful to both parties, provision might be built into the relevant scheme for a final sale of the name, assuming a fair price could be reached between the parties. Again, an even simpler alternative might be to create a permanent domain name sharing arrangement such as that suggested above in relation to competing legitimate commercial trademark interests corresponding to a given domain name. Such a system would not likely be too conceptually difficult to develop or require expensive litigation, as long as a suitable administrative mechanism could be established.

Of course, this mechanism might need to be limited to disputes between politician names and other personal names. Contests

337. See supra Part IV.D.4.
338. Again, the regulator, whether it is ICANN or some other body empowered by a relevant legislature, might assist in determining a fair price if the parties could not reach agreement. This could be similar to the scheme for assisting parties to establish fair licensing fees when they cannot themselves reach agreement. Such regulatory intervention in determining fair prices for sales and licenses of valuable intellectual property rights is not unprecedented. For example, in the United Kingdom, the Patents Act of 1977 contemplates government assistance in determining a fair price for the compulsory license of a patent in appropriate circumstances. See Patents Act, 1977, c. 37, § 48 (Eng.).
339. Unless, of course, the relevant policy was changed to encourage domain
between, say, trademarks and politician names may be more difficult given current domain name policy, although, presumably, such disputes would be rare in practice, because few politician names likely correspond to valuable corporate trademarks. It is more likely that a politician's name would conflict with a celebrity's name that has corresponding trademark rights. However, again, such cases would be rare, given that WIPO arbitrators, at least, have taken the view that, in most cases, only the highest levels of celebrity would give rise to corresponding trademark interests. In order to conflict with a politician name, not only would a celebrity name need to have achieved this status, but it would also need to correspond to the politician's name. This would be a very rare case, indeed.

F. Culturally Significant Names and Geographical Locations

A final potentially problematic category of domain name disputes involves domain names that correspond to more miscellaneous subjects, such as culturally significant names and geographical locations. This is a difficult area because the social and cultural norms that might be protected by granting legal rights in these names are probably harder to establish with any degree of certainty than those that might be protected with respect to trademarks and personal names. It may also be difficult to establish which people, groups, or government entities should have the strongest claim to a legal right in, say, a geographical location name or a cultural name linked with a particular geographical place or group of people. In the Report of the Second WIPO Internet Domain Name Process, WIPO recommended leaving domain name issues in these areas unresolved for further consideration. With respect to names of indigenous people in particular, WIPO suggested that further consideration could take place, including through WIPO's process of investigating intellectual property and genetic resources, traditional knowledge, and folklore.

A variety of difficult issues would arise in these areas if a property-rights regime, or something similar, was established for relevant domain names. Such rights may well conflict with other rights deriving from corporate and personal domain names. Thus, the matrix for resolving domain name disputes becomes even more

---

341. Second WIPO Report, supra note 102, ¶ 297.
342. Id.
complex when cultural and geographical indicators are added into the mix. An obvious example of where competing commercial, personal, and cultural interests may clash in one domain name could be the case of madonna.com. This domain name is currently registered to the pop singer Madonna.\textsuperscript{343} She has also registered "Madonna" as a trademark.\textsuperscript{344} She therefore has trademark interests in the name by virtue of the trademark registration, probably through common law trademark rights, and, perhaps, through celebrity rights in the name. However, the name clearly corresponds with other cultural interests, especially in relation to religious and artistic representations of the mother of Christ.

To date, the disputes involving the madonna.com domain name have revolved around competing trademark interests in the name, rather than cultural or religious interests.\textsuperscript{345} As noted above, the singer Madonna has registered trademark rights in the "Madonna" name.\textsuperscript{346} The madonna.com domain name was originally registered to a man called Dan Parisi in New York who had also registered the trademark "Madonna" under Tunisian law, expressly in order to defend any challenge by the singer to his domain name registration.\textsuperscript{347} Parisi admitted during the course of the UDRP proceedings that he only obtained the Tunisian trademark in order to protect his interests in the domain name.\textsuperscript{348} He was not located in Tunisia at the time, nor did he register the mark for the purpose of making any bona fide use of the mark in commerce in Tunisia.\textsuperscript{349} Parisi, presumably, chose Tunisian law because registration of trademarks in Tunisia proceeds without any substantive examination.\textsuperscript{350}

In a proceeding under the UDRP, Madonna received a ruling that the domain name be transferred to her on the basis that Parisi

\begin{itemize}
\item \textsuperscript{343} The domain name is registered to BoyToy, Inc., which is known to be affiliated with the pop singer known as Madonna. Network Solutions, \textit{WHOIS Record for madonna.com}, at http://www.networksolutions.com/whois/results.jhtml?sessionid=BZYT1TGH2QXEACWKEAQSFFA?whoistoken=0&imageKeyPage=/whois/entry.jhtml&_requestid=1430270 (last visited October 30, 2005).
\item \textsuperscript{346} See \textit{supra} note 344 and accompanying text.
\item \textsuperscript{347} Ciccone, Case No. D2000-0847, §§ 1, 4.
\item \textsuperscript{348} \textit{Id.} § 6.
\item \textsuperscript{349} \textit{Id.}
\item \textsuperscript{350} \textit{Id.}
had registered the mark in bad faith and had no legitimate interest in it.\textsuperscript{351} However, Madonna was in an unusually strong position in relation to other celebrity names because she had obtained a valid trademark registration of the name in the United States. As we saw in the preceding discussion, some other famous celebrities have had problems in this respect, with the \textit{Springsteen} arbitration as an obvious example.\textsuperscript{352} Thus, under this analysis, the \textit{madonna.com} example should fall into the class of domain names discussed first in this categorization scheme—domain names corresponding to valuable commercial trademarks. Madonna as an individual may have had less success under the UDRP had she not established registered trademark rights corresponding to her alleged common law rights in the word “Madonna.” Additionally, any other religious or cultural group interested in the name is unlikely to have any success in establishing rights in the word, given the fact that the singer’s registered trademark rights have now been successfully defended in a UDRP proceeding. None of this, necessarily, is meant to say that Madonna, the singer, does not have the best rights to the \textit{madonna.com} domain name. However, it does evidence the manner in which the domain name system has become skewed in its protection of trademark rights, particularly in cases where personal names are only effectively protected on a global level if they correspond to registered trademarks or powerful common law trademarks.\textsuperscript{353}

WIPO was probably correct in 2001 when it suggested that some of the more complex domain name issues require further scrutiny, consideration, and comment before any decisive legal and policy rules are formulated to deal with them.\textsuperscript{354} Geographical indicators and cultural references are likely the most obvious candidates for further consideration. However, it is important that consideration is given sooner, rather than later, and that a debate begins on global principles. Otherwise, we risk the very real possibility that commercial interests, and trademarks, in particular, will come to dominate all law and policy as it applies to domain names. It is possible that very real interests are being overlooked and will continue to be overlooked, unless the debate is refocused to

\begin{footnotes}
\footnotetext{351}{\textit{Id.} § 7.}
\footnotetext{354}{Second WIPO Report, \textit{supra} note 102, ¶ 297.}
\end{footnotes}
take account of some of these issues.

Various possibilities for legal reform exist, including: (a) mandated division of gTLDs so the same person or organization cannot monopolize different gTLD forms of the same name; (b) promotion of domain name sharing systems, in appropriate cases, in which two or more individuals or entities with similar legitimate competing interests in the same domain name jointly host the relevant Web site containing hyperlinks to their respective main Web pages on a permanent or temporary basis;\(^{355}\) (c) development of a compulsory licensing system to operate on a temporary basis and which might ultimately result in a final sale, in appropriate cases;\(^ {356}\) and (d) creation of a “veto” system for personal and, perhaps, also cultural and religious interests in relevant domain names, modeled on the restrictive covenant model from land law.\(^ {357}\) This would allow those with particular personal, social, or cultural interests in a given domain name to register impermissible uses of the name that would be binding on all subsequent registrants, without requiring the person seeking the veto to maintain registration of the name herself. The domain name “watch” services, “defensive registration” services, and “exclusion mechanisms” recently evaluated by the WIPO Arbitration and Mediation Center\(^ {358}\) may also have a role to play, particularly with respect to any new gTLDs introduced in the future, as well as specific iterations of domain names in existing gTLD spaces that have yet to be registered.

V. CONCLUSION

This Article has attempted to identify some of the more obvious social values we may consider promoting in a more expansive approach to domain name registration and dispute resolution. They include the protection of the policies underlying the trademark system, as well as the promotion of free speech on the Internet, the protection of personal privacy and public reputation, the prevention of political cyberfraud, and the facilitation of political communications more generally, particularly in the context of an election campaign. This is obviously a complex pastiche of social values that will need to be carefully balanced by policy makers as the system develops.

The above discussion has also suggested practical approaches that might be implemented alongside the UDRP and the ACPA to

\(^{355}\) As noted above, a temporary basis may be more appropriate for some political names.

\(^{356}\) See supra Part IV.E.3.

\(^{357}\) See supra pp. 159-161 and note 281.

\(^{358}\) New Generic Top-Level Domains, supra note 5, ¶ 23-25.
protect some of these values. In particular, it has advocated the adoption of a new classification scheme for different categories of domain name disputes that raise various different legal and cultural issues. This framework could be utilized in future development of domain name laws and policies in order to differentiate traditional bad-faith cybersquatting cases, which are adequately regulated under the UDRP and the ACPA, from other kinds of complaints regarding domain name registration and use. This would help in developing a more comprehensive domain name policy than is currently in use.

A new and more comprehensive policy may incorporate elements of the various suggestions made above in relation to resolving different classes of domain name disputes. Where competing legitimate interests are concerned, for example, ICANN could develop a domain name sharing policy, which could be facilitated privately by organizations like WIPO as a condition of domain name registration. Alternatively, national legislatures could adopt similar policies for these classes of disputes. Some competitions between legitimate interests might be resolved through temporary compulsory licensing arrangements, such as political versus private personal name disputes. Where two people have legitimate interests in a name and one is a politician, as in the kerryedwards.com situation, a temporary compulsory licensing agreement might be the optimal solution.

There are also those situations, as in the case of the juliaroberts.com domain name and, perhaps, also some cultural and religious words and phrases, where the complainant is not seeking to put to better use a particular name than the original registrant, but is, rather, seeking to restrict others from making an objectionable use of the name. These situations potentially lend themselves to the kind of veto system suggested earlier in this Article. This system could operate somewhat like a restrictive covenant system in a land title registry. ICANN or national legislatures could establish a mechanism for registering impermissible uses of particular domain names based on protecting personal reputation, personal privacy, or cultural or religious integrity in particular words or phrases. Alternatively, a domain name "watch" or "defensive registration" service might be introduced in the " .com," " .net," and " .org" spaces to protect personal and cultural names against unauthorized incursions.

359. See supra notes 318, 334-36 and accompanying text.
360. See supra notes 253-63 and accompanying text.
361. See supra Part IV.F.
362. See supra pp. 159-161.
363. These are all preventive measures as opposed to curative measures, but
A comprehensive domain name registration and regulation system incorporating all of these elements would certainly be more complex than the current system which mainly focuses on "classic," bad-faith cybersquatting, at least in the popular "com," "net," and "org" domain spaces. However, the time may have arrived to develop a more comprehensive approach to domain name disputes that is able to protect important interests in domain names, aside from those trademark holders already protected against bad-faith incursions by cybersquatters. WIPO may, ultimately, be correct in its opinion that international input is necessary in many of these areas in order to ensure that the ensuing policies and procedures adequately reflect emerging global norms, and such input will certainly take some time. Nevertheless, in contrast to WIPO and ICANN current priority lists, time may be of the essence in identifying relevant norms and in developing national and global mechanisms to promote important interests in domain names that currently are inadequately protected. Failure to do so in a timely manner will likely lead to an entrenchment of the notion that the only values worthy of legal protection, with respect to the most popular domain spaces, are those derived from traditional Western commercial trademark interests. If these are the only interests protected by national and global domain name policy, we risk the chance that the Internet will fail to reach its full potential as a global communications medium and, instead, be reduced to a bland, if convenient, commercial marketplace.