

11. Global Rights to Names

'Tis but thy name that is my enemy.

--Shakespeare, Romeo and Juliet

In Shakespeare's play *Romeo and Juliet* two clans, the Montagues and Capulets, are locked in a blood feud. Romeo, a Montague, falls in love with a woman of the Capulet family. His predicament causes him to muse on the significance of names – *'tis but thy name that is my enemy* – and he utters the famous line, “What’s in a name? That which we call a rose by any other name would smell as sweet.” But Shakespeare knew well what was “in” a name, even if Romeo did not. Although the names themselves were arbitrary, they were markers of powerful social boundaries. Whether you were tagged “Montague” or “Capulet” was a matter of life and death. In the end, the names won and the lovers lost.

Intrinsically, not much is “in” a domain name. Their value as locators, identifiers, and navigation aids is very much overrated. After being the focal point of global institutional change for more than six years, however, they are being made into territorial markers of great commercial and geopolitical significance. One of the most aggressive players in this drama is the World Intellectual Property Organization (WIPO). The once-obscure organization is trying to enter into a symbiotic relationship with ICANN, wherein WIPO provides the policy initiative for minting new rights in names and ICANN

provides the control points for implementing and enforcing them. The dirty little secret of the whole affair is that domain names are not nearly as valuable or as important as the new institutional regime would like to pretend they are. Domain name policy is really a proxy war. Extraordinary claims over the control of words and names are being advanced in the arena of Internet domain assignment because it is hoped (or feared) that it will set precedents for the treatment of the entire online economy. For WIPO and the intellectual property interests, the domain name space has become the site for this proxy war not because of its intrinsic importance, but because it is turf that can actually be controlled, due to the centralized nature of the root.

That all this weight is being placed on a system of computer identifiers that is distributed, hierarchically organized, and asks of names only that they be unique is one of the key weaknesses in the emerging regime. Never before has so much regulatory firepower been concentrated on a resource so ill-suited for the task. The attempt to vest the humble domain name with an increasingly regulated, official status would be comical if it were not so dangerous and costly. Nevertheless, this anomaly tells us something important about institutionalization processes. Institutions, once ensconced, can redefine technical systems to suit their own purposes, foreclosing technical possibilities and lines of business development that are inconsistent with maintaining the regime.

This chapter has two objectives. The first is to demonstrate that control of the DNS root is being used to create new and expanded rights to names. In the institutional response to the domain name - trademark interface, a common refrain is that the goal is only to preserve existing rights. But the property rights in names that are being created by

the new global regime are often stronger than, and always quite different from, traditional legal rights in names.

The second objective of the analysis is to demonstrate how ill-suited domain names are as a vehicle for advancing an expansive property rights agenda. Highly unrealistic assumptions must be made about the use and interpretation of domain names on the Internet in order to justify the new rights and the regulatory regime needed to enforce them.

11.1 A Web site by any other name....

On a computer network, identifiers are cheap, plentiful, and often playful. Names can map anything to anything. The costs of creating them and changing the mappings are low. The tradition of promiscuous and playful naming goes back to the Internet's origins in academia. Hosts were named after mythological figures (Thor, Zeus, Athena), characters from fantasy stories (Frodo, Gandalf, Rodan, Godzilla), or whatever else struck the fancy of the system administrators. Aside from the initial freedom to assign names, the anonymous interaction fostered by computer networks encouraged play in the adoption of user identities. The familiar joke, "on the Internet, no one knows you're a dog" encapsulates that reality. It is reinforced daily by experiences in chat rooms, public bulletin boards, and virtual worlds, where users can deliberately adopt and explore identities of their own creation. (Turkle, 1995; Lessig, 1999) Certainly there is a dark side to the ability to conceal or change one's identity in cyberspace. Sexual predators can use it to stalk children and securities hucksters can use it to unload stocks. Identity theft, spoofing and spamming are common problems. But the same technology that allows one

to define and alter the identity one presents to the online public also leaves behind so many trails and fingerprints that law enforcement still comes out ahead, except for a few skilled and professional culprits.

America Online, the most mainstream and commercialized of the big Internet service providers, understands the role of names in cyberspace. AOL provides each of its customer accounts with up to six screen names. The names are entirely user-selected, subject only to a uniqueness constraint and some limits on obscenity. With the exception of a primary name, the identities can be altered, adopted or deleted at will. Random searches of AOL's member list inevitably pulls up fun names. SexxyBone. Goofyrulzz. SugarMama84. Goofy4Ever. GretaGarbo18. (If someone else has already adopted the same name, numbers must be appended to it to make it unique; apparently, there are a lot of SugarMama and Greta Garbo wannabes on AOL.)

In the AOL name space, references to cartoon characters, movie stars, novelists, TV programs and other icons of popular culture are abundant. Not all are complimentary. In his user profile, AOL member "Fecking Goofy" lists his location as "the planet Pluto" and his hobby as "shagging Minnie." In open and free name spaces, as in real human interactions in conversation and physical space, people readily appropriate and incorporate into their own distinctive cultures references to "owned" names and characters. These conversations are more a reflection and reinforcement of the popularity and value of cultural icons than a dilution of them. To regulate such activity would destroy the point of it.

Usenet newsgroups are another example of a relatively free name space. Usenet is a way of organizing text-based discussion or file-exchange groups around specific topics,

and distributing them to users.¹ There is a group devoted to the collectors of Pez candy containers, for example, named *alt.collecting.pez*. The naming of Usenet groups is more like domain name assignment than the adoption of AOL user names. The names are hierarchical and point to content rather than individuals. (Of course, domain names also can be used exclusively for email.) Unlike AOL screen names, they are part of a public name space, and new ones can be assigned only after some form of collective action.²

Like AOL Screen names and user profiles, the Usenet name space commonly incorporates trademarked names. There is a newsgroup for people who hate Barney, the purple dinosaur character on children's television, named *alt.dinosaur.barney.die.die.die*. There is a *rec.arts.disney.parks*, a group not endorsed or operated by Disney, and a *rec.arts.tv.soaps.abc*. There is a *comp.os.ms-windows* newsgroup that is not operated or licensed by the Microsoft Corporation. Within the Usenet name space, it is commonly understood that names can refer to entities without pretending to be official, authorized versions of them.

In the domain name space, on the other hand, users are not allowed to claim that their name is Mickey Mouse and that they come from Disneyland. If anyone had tried to register *barney.com* or *barney.org* to run a web site for derogatory comments about the dinosaur character, the trademark lawyers would have pounced. And the American television network, ABC, has made it clear that it thinks it owns the common acronym "abc" under *any* top-level domain, as well as domain names such as *abc1*.³ Thus, an

¹ Usenet FAQ.

² Usenet FAQ description of how new groups are formed. (See HH 1990)

³ *Abc1.com* court case

interesting and fundamental discrepancy exists between the world of domain names and other computer naming systems. Why? It is *not* because the function of domain names is fundamentally different or more important than these other kinds of names. The differences stem from a combination of history and hysteria.

Chapter 6 described the explosion of domain name registrations under .com in 1995 and 1996 and the ensuing collision between domain name registrations and trademark rights. During that brief period, owning a simple domain name in the .com space was the equivalent of possessing a global (English) keyword. Many business people and intellectual property lawyers became convinced that domain names possessed a remarkable power to attract users and establish a global identity in cyberspace. This in turn provoked a concerted effort on the part of the intellectual property interests to make domain names a controlled vocabulary, and the data generated by a registration – known as WHOIS data – into an official record that can be used by intellectual property holders to identify and track down the registrant.

11.2 Expanding trademark rights

Throughout the domain name controversies, almost all sides of the dispute have reiterated the principle that new laws or policies should neither expand nor diminish traditional intellectual property rights. The Commerce Department White Paper claimed that its proposals “were designed to provide trademark holders with the same rights they have in the physical world.” (NTIA, 1998, Section 8) WIPO, too, made a point of emphasizing this claim:

“[T]he goal of the first WIPO Process was not to create new rights in intellectual property, nor to accord greater protection to intellectual property in cyberspace than that which existed elsewhere. Rather, the goal was to give proper and adequate expression to the existing, multilaterally agreed standards of intellectual property protection in the context of the multi-jurisdictional medium of the Internet.” WIPO 2, paragraph 18.

The notion that we are simply translating traditional rights into a new medium is easily exposed as fiction, however. The only way to do this would be to apply trademark concepts to domain name disputes on a case-by-case basis, using traditional legal standards and institutional methods. Instead, ICANN and its backers have directly inserted trademark protection criteria into the administration of the technical system. This is inherently problematical. Trademark rights are based on subjective criteria, involving factors such as interpretation, culture and confusion. Everything depends on the context and the way the name is used. Rights in the domain name system, on the other hand, are based primarily on technical exclusivity. Furthermore, trademark rights are territorial, whereas domain names are inherently global in scope. It is therefore impossible to map DNS administration and trademark protection onto each other without fundamentally changing the nature of the rights involved.

And we *are* in the process of altering the nature of name rights. Much attention has been devoted to the threat of cybersquatting. Less attention has been paid to the danger than measures to control it are expanding property rights to names at the expense of free expression, privacy, and competition.

11.2.1 *Mechanized rights*

Increasingly in the domain name space rights are established and defended not through *ex post facto* litigation that applies a legal standard to a particular situation, but by pre-emptive regulation. By “pre-emptive regulation” I mean techniques that protect name rights on an *ex ante* basis by hardwiring certain kinds of protection into the technical system. Rights become mechanized, the ultimate example of what Lessig (1999) calls regulation by Code.

The clearest examples of pre-emptive regulation are name exclusions. If one controls the root, one can insert into all contracts with domain name registries a list of prohibited names or words, and require all registries to check all applications for registrations against that list and block any registrations that match the words on the list. In other words, control of the DNS root can be exploited to make the assignment of certain names impossible, regardless of who uses them, the purpose of the use (e.g., commercial or noncommercial), or the impact of the use on the mark holder.

WIPO promoted the idea of across the board exclusions for major trademark holders during its first domain name process in 1999. (WIPO 1, 1999) It advocated creating a list of globally famous trademarks that would then be excluded entirely from the DNS database. The list of famous marks would be compiled by WIPO through an application and review process that did not impose any fixed limit on the number of companies or marks to be granted this exclusive status. The proposal was a rather dramatic contradiction of WIPO’s claim that it did not want to create new rights. An authoritative list of famous trademarks that is accepted on a global scale simply did not exist then, nor does it exist now. Had the ICANN process not blocked it, WIPO would

have created a completely new kind of name right and implemented it via the domain name space.

But WIPO is not the only organization to advocate and use name exclusions. ICANN's staff unilaterally imposed a significant number of name exclusions upon the new generic top-level domain registries it created in 2001. Most of the affected names were acronyms and names associated with the Internet technical community and ICANN's own organizational subsidiaries.⁴ Some of the excluded acronyms, however, were actually trademarked by private companies in various places in the world. The fact that global rights could be created by fiat, without any policy consultation or oversight, speaks to the potential power inherent in ICANN's position at the root.

Another form of pre-emptive regulation is simply the refusal to permit the creation of new top-level domains. Trademark holders fought successfully against the creation of any new TLDs from 1997 to 2000 because it would raise their policing costs and increase the possibility that someone, somewhere, might register a name that a trademark owner finds objectionable. If there are no new TLDs, that can't happen. Of course, there is no need to judge whether a particular registration really is diluting or infringing a trademark, either. The situation is analogous to what might happen if photocopying machines were banned, or access to them was tightly regulated by a copyright authority. Obviously, there would be fewer violations of the copyrights of book publishers and scholarly journal publishers. But all kinds of legitimate and legal activities would be curtailed, too.

⁴ ICANN-excluded names

There is of course nothing new about attempts by incumbent intellectual property holders to block the introduction of services or technologies that (they feel) threaten the exclusivity of intellectual property. Major copyright holders attempted to ban videocassette recorders on the grounds that someone might use them to make illegal copies.⁵ In those cases, American courts and legislators adhered to the common sense principle that one must not prohibit an entire business simply because a small portion of the activity it generates might be violating copyright or trademark laws. In the domain name space, however, intellectual property interests have achieved the kind of prior restraint that they have sought but never been given in other new communications media. Intellectual property holders have succeeded in gaining control, or a large amount of influence, over the point of market entry.

Pre-emptive regulation can also take the form of procedures regulating the initial assignment of names in new top-level domains. So-called “sunrise” procedures, for example, give trademark owners privileged access to domain name registrations in the opening phase of new top-level domains. A proposal put forward by the DNSO’s Intellectual Property Constituency, for example, demanded a 30-day period prior to the public launch of a new top-level domain during which registrations would only be available to trademark owners. The plan, dubbed the “Sunrise Plus Twenty,” allowed a trademark owner whose mark was at least one year old to register 21 variations of a trademarked name within the new TLDs. It also asked registries to supply these “sunrise” registrations at a discount to normal domain name registration fees. Such procedures privilege trademark owners over other claimants regardless of whether classical

⁵ (Sony case)

infringement is involved. This is a brand new kind of trademark right; such pre-emptive privileges over the adoption of names by presumptively innocent third parties have never existed before. Indeed, the rights created by both the famous marks exclusion and the Sunrise-plus proposals are so far afield of traditional trademark rights that they would bring many legitimate trademark holders into conflict with each other. Although the extreme version of sunrise sought by INTA and other large trademark holders was not implemented, many of the new TLDs licensed by ICANN did adopt milder variants of the “sunrise” proposal. Indeed, even the new *.name* top-level domain, which was supposed to be devoted exclusively to individual domain name holders who wanted their domain name to reflect their personal identity, adopted a sunrise procedure.⁶

The problem with name exclusions, sunrise proposals and other pre-emptive rights should be apparent. They substitute technical exclusivity and *ex ante* rules for what should be *ex post* legal judgments. Hence, they are completely insensitive to the boundaries and limitations that normally accompany trademark rights. Limitations on the ownership of words and names meant to protect freedom of speech and fair use can easily be squashed in a regime based on technical exclusivities. An across the board name exclusion doesn't distinguish between the name *ford.sucks*, which might be used legitimately for a protest site about the automobile company, and a deceptive or infringing registration of the domain name *ford.com*. It cannot make a distinction between the many legitimate concurrent uses that might be made of trademarked words, such as the Ford Theatre, the Ford Modeling agency, and the Ford Motor Company.

⁶ Reference to *.name* sunrise procedure

Neither WIPO nor the trademark interests have succeeded in getting all the preemptive rights that they wanted out of the new regime. But it is more significant is that such rights are constantly being sought, and that it is fairly easy to implement them as long as artificial scarcity is maintained and ICANN continues to link technical coordination to policy making. The new regime encourages and rewards such expansion. Fighting against it, on the other hand, is costly and difficult.

11.2.2 Expanding surveillance rights

A critical part of maintaining any property right is the need to monitor its boundaries; i.e., to identify perceived violations of the right and take effective enforcement action against them. Under traditional trademark practice, the owner of a mark is responsible for all policing and monitoring activity and costs. In the physical world, there is no single, integrated, global database of company, product or brand names in which everyone must register. Trademark policing relies on a variety of activities: monitoring official trademark registers, checking telephone directories and yellow pages, searching industrial directories, and physically examining products in stores, to name a few. A number of specialized firms supply this surveillance function on a commercial basis to major brand holders.

As discussed in Chapter 9, the creation of an institutional regime based on control of the DNS root has made it possible for intellectual property interests to claim new and expansive rights of surveillance over the adoption of names by users. The vehicle for these new rights is the WHOIS database.

The WHOIS database allows one to type in a domain name and pull up the name and address of the individual or company that registered the domain. It also shows the

dates on which the domain was created, when it expires and when it was last updated. It includes the name, address, and contact numbers of the domain technical administrator, as well as technical information, such as the domain name and IP addresses of the name servers that are used to resolve a name. The protocol was invented by the original creators of the Internet to provide information that might be needed to resolve technical problems involving a domain or an IP address. Later, the information proved to be useful in tracing the source of spam or hacking attacks. As domain names became economically valuable, WHOIS also became a popular way of finding out which domain names were taken, who had registered them and when, and when the registration would expire.

With the emergence of domain name – trademark conflicts, the WHOIS protocol took on a new function. It became a surveillance tool for the intellectual property holders. The IP interests discovered that they could perform searches for character strings that matched trademarks, and pull up many of the domain name registrations in the generic top-level domains that matched or contained a trademark. This automated and universal searching function proved to be so valuable to the trademark interests that they began to demand that the WHOIS surveillance functions be institutionalized, expanded, and subsidized.

The first WIPO process recommended that the contact details in a WHOIS record be contractually required to be complete, accurate, and up to date, on penalty of forfeiture of the domain name. (WIPO 1, para. 73) The intellectual property interests also demanded “bulk access” to the WHOIS data of domain name registrars; i.e., the right to purchase the complete list and contact data for all of a registrar’s customers in one fell swoop. They now want WHOIS functionality to be expanded, so that data can be

searchable by domain name, the registrants' name or postal address, technical or administrative contact name, NIC handles,⁷ and Internet Protocol addresses. They also want searches to be based on Boolean operators or incomplete matches, as well as exact string matches. Further, they are requesting that the results of searches not be limited to a certain number (Network Solutions can only return 50 records at a time). Moreover, they want this expanded capability to be subsidized; i.e., they want it to be considered a part of the public Internet infrastructure and not a value-added service that they would have to pay for. Not content with the already massive reduction in transaction costs brought about by the mere existence of a single, integrated name space that can be searched using automated tools, they want to shift the costs of policing and monitoring the trademark-domain name interface onto users, registries, and registrars.

As noted in Chapter 9, the issue is no longer exclusively one of trademark surveillance and protection. Copyright interests now view expanded WHOIS functionality as a way to identify and serve process upon the owners of allegedly infringing web sites. That is, "technical coordination" of the domain name system is already being leveraged to police the *content* of web sites, as well as their domain names. Moreover, public law enforcement agencies, notably the U.S. Federal Bureau of Investigation (FBI) have become deeply interested in the use of WHOIS to supplement their law enforcement activities. Ultimately, the intent seems to be to make a domain name the cyberspace equivalent of a driver's license. Only unlike the drivers' license

⁷ The NIC handle is a short, unique alphanumeric code that a registry assigns to a domain name holder when the registrant registers a name. People who use different names might use the same NIC handle in the WHOIS record.

database, this one would be publicly accessible to anyone and everyone to rummage through as they pleased.

Whether one supports or opposes the intellectual property interests' agenda for the WHOIS service, it is incontestable that the surveillance rights they are seeking are more comprehensive than any that have existed before. A reduction of transaction costs per se is not bad; indeed, from an economic standpoint lower transaction costs, almost by definition, contribute to greater efficiency. The problem is that the expansive and compulsory WHOIS functions sought by the intellectual property interests do not reduce transaction costs for all. They mostly shift cost and risks that used to be assumed by intellectual property owners onto end users, registries, and registrars, in order to make life easier for trademark owners. End users are being asked to sacrifice privacy and expose themselves to spam, slamming, and other unsavory practices that exploit the open availability of WHOIS data. Registrars are required to lose control of their customer lists. Both registries and registrars must make major investments in software and infrastructure to support the comprehensive global surveillance capabilities sought by the intellectual property interests.

To compel everyone in the domain name space to expose themselves to surveillance expands the strength and comprehensiveness of an intellectual property owners' rights over names. To require that the system be funded by the subjects of the surveillance is the *coup de grace*.

Just how radical a shift in the balance of power the IP agenda for WHOIS represents was illustrated by an amusing exchange on a public email list between Judy Henslee, the US trademark manager for Harley-Davidson motorcycles, and an intellectual

property lawyer, John Berryhill. Ms. Henslee was complaining about the limitations of the current WHOIS protocol on the INTA email list, and concluded “the ability to produce (or at the very least, purchase) accurate lists of all domains owned by a single person or entity would be extremely helpful to the trademark owner.” Mr. Berryhill replied:

Dear Ms. Henslee,

I was sitting on my back porch this evening, and someone drove by riding a Harley Davidson motorcycle with a defective exhaust system. My community has strictly enforced noise and smog ordinances, and this person was clearly in violation of both. This person was also not wearing a helmet, in violation of the law. I shouted at the rider, whereupon he rode across and damaged my lawn.

I would like to bring a trespass action against him, but I could not identify him. However, I can identify the make, model, year and color of the hog.

I went to your website, and I noticed that Harley Davidson does not provide a readily accessible database of warranty registrations or, indeed, any other information that will assist me to identify the violator. As you surely can appreciate based on your comments concerning the WHOIS database, your provision of this information would certainly help in bringing this lawbreaker to justice, as well as anyone else who uses a Harley Davidson product to violate the law. As I'm sure you are aware, despite the fine reputation enjoyed by Harley,

and my own admiration for your machines, there is an element of the subculture associated with your company's product which has been known to demonstrate a pattern of unlawful behavior such as gang activity and drug transportation. Many of them may own more than one motorcycle. So, I'm sure there is considerable demand for this data.

Since there doesn't appear to be a convenient database, is there some way that I can arrange to purchase the names, postal addresses, email addresses, and telephone and fax numbers of people who own Harley Davidson motorcycles? If I send the description to you, will you help me identify the owner?

The Harley-Davidson lawyer was not amused by the parallel. But she did not argue effectively against its validity. Under ICANN's contractual regime, the consumers and suppliers of domain name registration services are required to facilitate their own surveillance by intellectual property owners. If we apply the same logic to any other industry, it seems absurdly overreaching. Motorcycles can be used to break the law, but we do not require all vehicle manufacturers to create a publicly accessible, global database with complete and accurate contact information about all their customers. Even the official, state-issued licenses attached to such vehicles are not open to anyone who wants to search through them; one must go through official law enforcement channels and demonstrate some cause of action. The linkage of resource administration to policy and regulation in the domain name regime has given intellectual property interests much more extensive rights of surveillance than they had before.

11.3 New rights in names: WIPO 2

If there were any doubts about the intent of WIPO and certain other interests to take advantage of the ICANN regime to create new rights in names, they were resolved with the release of the Interim Report of WIPO's second domain name proceeding. (WIPO, 2001) The second WIPO proceeding advocated several new types of name exclusions and some modifications of the Uniform Dispute Resolution Policy to recognize new rights in domain names. The new rights involved names of international organizations, non-proprietary pharmaceutical names, geographical indicators, country codes, personal names, and trade names. The new rights were proposed before ICANN had even begun to evaluate its uniform dispute resolution policy.

11.3.1 *INNs and IGOs: taking care of your own*

One of the focal points of WIPO's report was the list of International Nonproprietary Names for pharmaceutical substances (INNs) created by the World Health Organization. The INN list consists of 8,000 generic names of drugs, such as "ampicillin" or "penicillin." Over 100 new names are added to the list each year. The purpose of the list is to ensure that no one can claim proprietary rights to those terms. The INN list, therefore, is intended to preserve freedom of expression in the realm of drug development and medicine by ensuring that no company or individual can control or regulate the basic terms used to scientifically describe and define pharmaceutical substances. One would think, therefore, that those terms' use in the domain name space would be open to all, as it is in other contexts. The World Health Organization is concerned, however, that the registration of an INN as a domain name means that a

private interest might “control” an INN. Indeed, it refers to the registration of a domain name as a “monopoly of association.”

Monopoly? WHO’s understanding of DNS is less than perfect. It does not seem to understand that an INN can show up in any one of more than 257 top-level domains; that the number of TLDs could be expanded to a million; that INNs could show up in third-, fourth, and fifth-level domains (or further down the hierarchy) or on the right-hand side of a URL. In fact, the report admits that “evidence of actual damage resulting from the registration and use of INNs as domain names is lacking.” (WIPO 2001, paragraph 45)

None of these facts deterred WIPO from proposing to mint a new global right. It recommended that all character strings identical to INNs, in five official languages, be excluded from the DNS database. WIPO would like the exclusion to apply in all open generic TLDs, and urges all ccTLDs to adopt it, too. Moreover, it proposes to expropriate holders of existing registrations by canceling their domain name registrations.

The WIPO report also recommends special treatment of the names of international intergovernmental organizations (IGOs). Under current treaties, IGO names are protected against registration of their names or acronyms as trademarks or service marks. WIPO proposed to exclude the exact names and acronyms of official IGOs from all gTLDs, regardless of how they were used. As in the case of INNs, it did not document a significant social problem caused by abusive registration of IGO names. Indeed, the only statements in support of the exclusion came from the IGOs themselves. The comment below, submitted to WIPO by the Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization, was typical of the rationale put forward:

“[I]t is important to have only one, authentic source of information in the Internet and to prevent the establishment of competing, unofficial Internet sites that may contain misleading, inaccurate, or prejudicial information, or that may lead the viewer to believe that he or she is using the official web site of the organization.”

This statement makes it abundantly clear that by regulating DNS labels, we are regulating speech and content as well. The treaty organization cited above wants to leverage the administration of DNS to ensure that there is “only one, authentic source of information” about itself on the Internet and to prevent the formation of “competing, unofficial” sites. Few would object to measures aimed at eliminating fraudulent or deceptive web sites, whether they target international organizations or any other type of organization. But fraud of that sort does not require a global name exclusion ; it can be addressed by existing treaties and by the existing Uniform Dispute Resolution Policy. A more likely scenario is that the names of IGOs would be used not by frauds but by parodists or political critics to operate web sites with critical or humorous content. An across the board exclusion seems intended only to prevent these critics from attracting the attention of the public by incorporating the IGO’s name in to their domain name label.

11.3.2 Geographical designations

Geographical designations include the names of cities, nations, regions, or locations. Often geographic names are used as indicators of the source of agricultural or manufactured products. Because of this type of usage, an extensive body of intellectual

property law has grown up around them.⁸ But neither the geographical indications themselves nor the legal principles governing them are uniform across territorial jurisdictions. As one legal scholar put it, “The same word can, in different contexts, constitute fully or partially a geographical indication, an indication of source, a geographic term, a descriptive term, a personal name, and a trademark. In other words, merely because a certain word functions as a geographical indication in one market, jurisdiction, and language, does not mean that the word is inherently a geographical indication.”⁹ Terms such as “champagne” or “bourbon,” which have specific and regulated applications in France, may not be protected at all in the United States.

Nevertheless, the second WIPO report recommended the adoption of new measures to protect geographic indicators and indications of source in the open top-level domains. It proposed to do this by broadening the scope of ICANN’s Uniform Dispute Resolution Policy (UDRP) to include abusive registrations of geographical indications and indications of source. The result of such a move would be to vastly complicate the definition and application of the UDRP, and to foment hundreds if not thousands of new disputes as different territorial norms began to collide with each other. Even the

⁸ The Paris Convention, Article 10(1) states that its provision on seizure of goods traded across national boundaries shall apply to instances where false indications of the source of the goods or the identity of the producer are used. The Madrid (Indications of Source) Agreement broadens the application of the Paris convention to “deceptive” indications of source. The Lisbon Agreement regulates “appellations of origin,” requiring participating states to protect registered appellations against any “usurpation or imitation.” Geographical indications are also covered by Articles 22 and 23 of the TRIPS Agreement.

⁹ Christine Haight Farley, Assistant Professor of law, American University, Response to the Interim Report of the Second WIPO Internet Domain Name Process, Washington DC Regional Consultation, May 29, 2001.

International Trademark Association recognized that extending the UDRP to geographical terms would require “extensive adjustments” in the UDRP’s language. “The number of required amendments would transform the UDRP from a relatively easy-to-understand process to a more complex legal regimen that may not be readily understandable, especially to respondents who are presented with a cause of action against them.”¹⁰ It is difficult to understand why WIPO would propose this other than as part of an ambitious attempt to exploit the leverage of the domain name system to carve out a new global system of name rights with itself at the center.

It is interesting to speculate on what would have happened had WIPO’s proposed regime been in place back in November 1994, when a start-up company with no real connection to Brazil registered the name *amazon.com*. Most likely, the claims of a small US company with no political clout would have been brushed aside as an “inauthentic” use of an important geographical indicator.

11.3.3 *Rights of personality*

Common pool conditions in the domain name space allowed anyone to register personal names as well as trademarked product names. Entertainers, celebrities, politicians, and some not-so-famous people found that their names had been registered by someone else. Frequently they did not like the use to which it was put. One activity in particular got the attention of politicians: the registration of the names of elected politicians and political candidates as domains. The names became the address of

¹⁰ Letter from International Trademark Association to Francis Gurry, May 24, 2001. Available on WIPO site in comments on RFC-3, Second WIPO process.

websites critical of the candidates' political views. Or they were offered to the candidates for a higher price.¹¹ While the Republican and Democratic parties' national committees expressed valid concerns about the use of domain name registrations to extort payments from campaign committees, they also raised troubling issues about the overlap between domain name regulation and free expression. The Democratic Party's national committee, for example, complained about the "voter confusion arising from a multiplicity of sites with domain names including the candidate's name, when such sites are created by individuals or organizations in order to criticize or parody the candidate, rather than for profit." Was their concern really the abusive registration of names, or simply a desire to make their political opponents and critics a bit harder to find?

Because of the power of Hollywood, strong national legislation in the United States has already addressed personality rights in the domain name space. The so-called Anti-cybersquatting Consumer Protection Act (ACPA) allows civil lawsuits against people who register the domain name of a person "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." Even before ACPA, several US court cases stripped domain name speculators of registrations of the names of celebrities and performers.¹²

In general, personal names are not protected as marks unless they are used and/or registered as an identifier of a product or service. There are laws against defamation, libel, and slander, but they pertain to content rather than labels. Within the ICANN

¹¹ Terry Allen, "Squatting for dollars: A political cyber-squatter makes mischief, and a few dollars, by registering candidate domain names." [Salon.com](#), June 12, 2000.

¹² Law cases on personality rights

regime, several UDRP decisions have recognized and upheld personality rights when the name in question is associated with famous performers and effectively functions as a trademark.¹³ The results, however, are mixed. Several cases uphold the right of third parties to register someone else's name if they are fans or have something to say about the person and wish to identify the site using a direct nominative reference.¹⁴

The second WIPO process considered some of these issues and raised the possibility of amending ICANN's dispute resolution policy to strengthen personality rights. The new right WIPO proposes would apply when the name is distinctive and the domain name registration is commercially exploited by an unauthorized party. The definition of "bad faith registration" would be modified to include practices that take advantage of the reputation or goodwill in a person's identity. The WIPO wording does not sound all that unreasonable, but it constitutes yet another step in the direction of an expanded, global regime of rights to names with WIPO at its center. The Report was weak in documenting abuses, and particularly weak in demonstrating that the abuses that exist in this area are not being handled by existing remedies. If the UDRP is modified, thousands of new disputes will be created, as people around the world would be encouraged to bring claims against anyone who registers their personal name as a domain name. There are no guarantees about the results of a UDRP case, so the risk of registering such a name will rise. "Taking advantage of the reputation or goodwill in a person's identity" can be an all-encompassing claim. If someone writes a book about a famous

¹³ Julia Roberts, Beatles UDRP Cases

¹⁴ Springsteen. SkipKendall

person and uses the name in the title, are they taking advantage of someone else's reputation? Probably so.

11.3.4 *Country names: semantics and sovereignty*

An especially potent subset of the controversy over geographical designators concerns country names, including both the words themselves and the two-letter country codes of the ISO-3166-1 list. In this case, the rights being asserted are not derived from commercial trademark rights, but are put forward as extensions of national sovereignty.

The ISO list of country codes embodied the pre-Internet international communication regime. It reflected a world of territorial nation-states where international relations were coordinated by treaty-based inter-governmental institutions. By incorporating this artifact into the domain name space, Jon Postel inadvertently helped to reproduce the political geography of the *ancien regime* in cyberspace. The ISO codes were originally part of a private name space, and were intended to be nothing more than an identifier of what country a domain administrator was in. Remarkably, these casual delegations of top-level domains were transmuted into the basis of a sovereignty claim by national governments. According to the ICANN Government Advisory Committee, the “relevant national government or public authority” should determine who receives the right to operate a country code registry, the duration of the license, and any review or revocation processes.¹⁵ This claim should not be confused with the simple and unexceptional notion that a registry located in a country must conform to the law of the

¹⁵ GAC, Principles for the Delegation and Administration of ccTLDs, 23 February, 2000, Section 9.

country. Rather, nation-states via GAC are claiming that they should have the authority to determine who is *assigned* the country code top-level domain for their country. That is, they are asserting a right to share with ICANN the power to make top-level delegations. The claim is based on the flimsiest of grounds: an arbitrary semantic relationship, the notion that the ccTLD string “stands for” or “represents” the country, and that that semantic relationship is somehow exclusive and privileged. In fact, there could be many different TLDs referring to a specific country (e.g., *.us*, *.usa*, *.america*, and so on). The arbitrariness of the relationship becomes evident from ccTLDs such as *.tv*, *.cc*, or *.md*, which exploit the semantic properties of their country code to generate domain name registration business unrelated to the country itself, and which contract out the registry operation to companies in the US or Britain.

But political factors have overridden technical and business facts in this case. The GAC has lobbied to make sure that ccTLD delegations are exclusive by warning ICANN not to delegate any new TLDs with the names of countries or that use the three-letter country codes. ICANN President Mike Roberts expressed support for the idea of giving governments the opportunity to register or assign in advance the two-letter and three-letter ISO country codes in the new TLDs.¹⁶ In its second process WIPO proposed to exclude all two-letter country codes from the second-level of all new generic TLDs.

Elizabeth Porteneuve, an adviser to France's *.fr* registry, said that ccTLDs are “attached to the reputation of the country. It's important, like a brand name.”¹⁷ The

¹⁶ Mike Roberts to Verrue, 1 December 2000. ICANN web site.

¹⁷ Kenneth Neil Cukier, “Governments stake claim for control over country-specific domain names,” Communications Week International, 7 June 1999, page 1.

government of the Republic of South Africa has taken an even stronger stance. It has objected to the common practice of registering country names in the second-level domain space, when the registrants “have no association or tie with that country.” It goes on to say that:

It is the position of the Republic of South Africa that second level domain names the same as Country Names are valuable national assets belonging to the respective sovereign nations. The country names in the gTLDs, particularly the dot-com TLD, have the potential to be of substantial political and economic value, particularly to developing nations.¹⁸

Clearly, by adjusting the UDRP to recognize geographical indicators, WIPO opens the door to claims that *any* registration of the name of a country is “abusive.” As the WIPO report recognizes, the same logic could also be used to support protecting the names of provinces, counties, cities, towns, and national parks. It also raises, but does not resolve, questions about rights to register the names of sub-national groups, ethnic groups, and the names of tribes or indigenous peoples.

One can only wonder when the demand for protecting religious terms will surface. The current regime offers exclusive protection for the names of cookies, laundry detergents, and thirty-six different misspellings of “Yahoo.” But it allows sacred names and profound concepts to be appropriated by anyone who wants them. Shouldn’t our regulatory apparatus make sure that the registrant of *allah.org* (or its equivalent in Arabic

¹⁸ SUBMISSION BY REPUBLIC OF SOUTH AFRICA IN RESPONSE TO WORLD INTELLECTUAL PROPERTY ORGANISATION'S WIPO2 RFC-2 PROCESS, March 1, 2001.

script) is a devout Muslim, that *jesuschrist.com* is in authentic hands,¹⁹ that the registrant of *truth.com* lives up to the name?

11.4 Free Expression vs. Controlled Vocabulary

At the heart of the controversy over global rights to names are two distinct and incompatible ideas about domain names and the function of the domain name system (DNS).

One view sees domain names as a highly flexible naming framework that gives users tremendous freedom to adopt names and naming conventions, and use them to express and advertise messages and identities in a public space. In this view, the DNS protocol is just a framework for coordination. It is the users who autonomously select the names and give them meaning through their uses; the protocol merely ensures that they are unique. The naming regime this produces has no overall organization – it is self-organizing – and offers no guarantees of authenticity. The results are sometimes confusing. But the system as a whole leaves room for creativity and innovation and, more

¹⁹ In a rather delicious irony, *jesus.com* has been registered by a Washington DC-area man with an uncanny resemblance to the stereotypical Bible-school picture of Jesus. The web site at that address is an extended personal ad: Golden-haired, blue-eyed Jesus seeks loving young woman (22-29), preferably of recent Norse-Germanic heritage, who wishes to live in the spirit of the eternal. Innocence, or rebirth into innocence, and a desire to transcend the material mendacity of this world are essential! I offer a pure and spiritual existence of life's essence, free of fear, free of despair. I will reveal the bliss, power, and endless rewards of faith and belief. The right woman who is ready for my love, blessings, and unforgettable spiritual exploration will be given the world, but will also want to give me her world in the mutual quest to share the infinite. I offer you the ability to experience the fulfillment of your dreams and all you seek. Prospective respondents should read 1 John 4:18. True to artistic depictions, I have a lean swimmer's body and a six-pack, and if you have sought your best in life you will also be in good shape. Where is WIPO when we need it?

importantly, is highly responsive to what the broad masses of Internet users want to do with names. It was this freedom, after all, which created the global market for domain names.

The opposing view – the one that animates WIPO and other international organizations, many trademark holders, and national governments – strives to make domain names into what information scientists call a *controlled vocabulary*. A controlled vocabulary is a system of classification and naming wherein each term has an official and precise meaning. A controlled vocabulary presupposes an authority with the ability to make binding determinations as to what names are associated with what entities. The Library of Congress index or scientific taxonomies for classifying plants or chemical elements are examples of controlled vocabularies. As the examples suggest, controlled vocabularies can be extremely useful for a specific purpose. They are also rigid and constraining, and cannot be used successfully for anything other than the purpose for which they were designed.

Which approach to domain names – coordinated free expression or controlled vocabulary – is better suited to the Internet? Below, I argue that the DNS protocol answers this question for us. The DNS *is* a system of coordinated free expression; it cannot be made into a controlled vocabulary without drastically altering its functions.

11.4.1 *Seven Assumptions*

The effort to turn domain names into a controlled vocabulary is founded on a series of assumptions about how domain names are used, what they signify, and how they are interpreted by ordinary Internet users. Those assumptions are listed below. (The

supporting commentary and footnotes refer to legal decisions and statements that show that these assumptions are widely held and commonly asserted.)

1. The DNS is a Directory

This assumption posits that the purpose of DNS is to guide users to specific kinds of content, web sites, or services. As a corollary, end users search for what they are looking for on the Internet primarily by consulting lists of domain names or by guessing domain names.

2. Authenticity

Domain names are (or should be) “authentic.” To possess a domain name is to possess an official, authorized relationship to the named person, place, organization, or thing. A stronger form of this assumption holds that for any given name, it is possible to know which applicant has the most valid claim to it.

3. Hierarchy doesn't matter

Domain names are not really hierarchical. It does not matter whether a character string is registered under .com, .to, .net, .org, .blat, .xxx or anything else. A name must be protected in ALL top-level domains otherwise it has no meaningful protection at all.

4. Non-uniqueness

Domain names need not be unique. If a registered name looks something like a name that someone has rights to, including misspellings or words in combination with a trademark, then it ought to be held by the rights holder, or at the very least not held by someone else.

5. Domain names are trademarks

Every domain name points to an e-commerce web site, an offering of goods or services. Domain names are not used to express ideas or refer to things.

6. Domain names strongly influence content interpretation

Internet users' interpretation of what they encounter on the Internet and the Web is closely linked to the semantics of the domain name. Thus, if a domain name address leads users to information or content different from what they expected to find, they will be hopeless confused. As a corollary, in adjudicating domain name disputes the actual content of a web site is not as important as an analysis of the text of the domain name itself and whether it can be construed, in isolation, as somehow impinging on the scope of a mark.

7. Global visibility

The mere registration of a domain name guarantees the registrant a substantial public audience. The name or site does not have to be advertised or promoted to have a significant impact; indeed, it does not even have to be visible on the Internet or associated with an operational website or email account. Millions of users will

spontaneously type the name into their browsers, without any prompting or advertising.

All of the above assumptions are problematical. Many are simply false. Some are half-truths, while others stand in direct contradiction to how domain names function technically. Taken together as a package,

Consider first assumptions #1, #2, and #6: that the DNS is a directory, and the purpose of the directory is to steer users to officially sanctioned information correlated with the name. This set of assumptions is the most fundamental one behind the push to make DNS into a controlled vocabulary. It is embedded in many court decisions and UDRP decisions. The second WIPO report boldly states that:

“The placing on the domain name register of a distinctive name, such as *gretagarbo.com*, makes a representation to persons who consult the register that the registrant actually is, or is associated with, the person whose name is registered and thus is entitled to use the goodwill in the name.” (WIPO 2, paragraph 139)

This view of domain names is fundamentally inaccurate. The WIPO statement, for example, contradicts what we have already established about users’ adoption of identities on the Net. The many AOL users who chose some variant of the name Greta Garbo are making a statement about *themselves* – their personality, likes and dislikes –

not representations to others that they *are* Garbo. Nor is it likely that many users who see the name interpret it as such, given the context.

Moreover, the theory that the DNS is an authoritative directory reveals a basic ignorance of how the protocol actually functions. People do not find things on the Internet by “consult[ing] the register” of domain names.” The domain name “register” consists of resource records scattered around half a million nameservers in different parts of the planet. To compile and “consult” that list, one must pull out zone files using complicated software. Even if it were possible to do so, the list one consulted would consist of nearly *40 million* second-level domain names; the *.com* zone file alone would contain over 23 million. That simply is not how ordinary users find things on the Internet. The notion that domain names are used for “searching” confuses searching techniques with locators, two completely different functions.

When users type in a domain name to locate a site, it is usually because they already know the domain name and the nature of the site they are headed to. That is, they are trying to *locate* the site. Although some users try to find sites by guessing an organizations’ domain name, it is done as a last resort after other methods have failed. The vast majority of users rely on search engines and portals. They locate content through hyperlinks that they receive from email or see on other sites. They bookmark links in their “favorites” file. Or they copy down or remember specific names that they have seen advertised.

As for assumption #6, type the words “Greta Garbo” into the popular Google search engine and one gets over 38,400 hits. Interestingly, *none* the top ten listings that are returned by Google have domain names that include the labels “gretagarbo,” “garbo”

or “greta.” The URL that arrives at the top of the heap is www.mdle.com/ClassicFilms/FeaturedStar/star53.htm, a tribute to Garbo put up by a fan club for silent movies.²⁰ Likewise, on Yahoo and Hotbot, the most highly ranked content on Garbo is under domain names like *netcomuk.co.uk*, *home.hiwaay.net*, or bombshells.com. In the majority of cases, there is no correlation between the content of a web site and the semantics of the domain name. At *gretagarbo.com*, on the other hand, ownership appears to rest in the hands of Garbo’s heirs or licensees. At that site one finds a rather slow and poorly organized site selling jewelry. Although the connection to Garbo is “authentic,” is it fair and valid to assume that anyone using Greta Garbo as a keyword or domain name is looking for that particular line of jewelry?

Users who employ Greta Garbo as a keyword may be interested in communicating with other people who are fans of Garbo. They may want to buy a book about her, find a picture of her, or find out which retail stores sell copies of her movies. For all we know, a user may be trying to find out whether MTV has produced an episode of *Celebrity Death Match* (a cartoon using animated clay figures) that pits Garbo against Madonna. Given what we know about the Internet and the incredible variety of content and materials available there, it is presumptuous to claim that we *know* what people who type names into their browsers are looking for. There are at least as many different objectives for searches as there are searchers.

Consider next #3 on the list. It is a fact that DNS names are hierarchical. Nevertheless, the assumption that the semantics of the top level do not matter is

²⁰ The domain name in this URL, *mdle.com*, refers to M. David Lewis Enterprises, an organization that has no official relationship to Garbo or her estate.

becoming an increasingly common part of the jurisprudence of domain name law and the UDRP. If one has a legal right to a name in one TLD, the theory goes, that right should extend across multiple TLDs, because users cannot be expected to differentiate among different top-level domains.

WIPO used this argument to support its policy of name exclusions for international organizations. A special top-level domain, *.int*, is reserved for legitimate international treaty organizations. WIPO recognized that Internet users “can have reasonable confidence and trust as to the genuine identity of the organizations registered in *.int*, and of the validity of the information provided by those organizations.” (WIPO 2, para. 102) The WIPO report also argued, however, that the mere existence of valid registrations in the *.int* domain is not sufficient because abusive registrations can still take place in other top-level domains. In essence, WIPO is arguing that the top-level of a domain name doesn’t matter. The same assumption shows up frequently in UDRP cases and domain name litigation. In one well-known British case, a judge took away the *bt.org* domain name from speculators and awarded it to British Telecom even though BT already had the *bt.com* domain and the acronym BT could be used by many different legitimate organizations.

The assault on hierarchy is now being pushed into the second and third levels. The second WIPO report, for example, argued for excluding country codes from the second level on all new top-level domains, because users are unable to distinguish between domain names like *company.uk.com* and *company.co.uk*. And some trademark hawks are beginning to seek to assert rights in third-level delegations.

Consider next assumption #4. Uniqueness is the most significant requirement of domain name assignment under the standard protocol. But to DNS, “unique” means any difference in a character string that can be recognized by a machine. Uniqueness to a machine is not the same as differentiation by a human. Humans might use any one of several different names to denote an organization, idea, or product, and they may not be able to distinguish between different spellings of the same word. In response to this problem, many brand holders have attempted to register every possible permutation of their name, multiple misspellings, as well as domain names that include the trademarked term along with generic terms, such as *fordcars.com*, *fordmotors.com*, *ford-source* and so on. Both UDRP panelists and courts have often upheld their right to reclaim such domains.

Here again, however, the desires of trademark owners are fundamentally at odds with the nature of DNS. The protocol allows any unique character string to be registered. It does not care whether the names appear similar to humans. The giant telephone company Verizon, formed via a merger of GTE and Bell Atlantic, learned the futility of resisting DNS’s reliance on uniqueness. Just before announcing its merger and new name, Verizon purchased close to 500 domain names, including not only *verizon.com* and *verizonlongdistance.com*, but also *verizonsucks.com*, and several misspellings of the brand. Later, the publishers of the hacker magazine *2600* tried to register *verizonsucks.com* to operate a site for consumer venting. Upon discovering that the name was not available they registered *verizonreallysucks.com*. The humorless telephone company sent them a cease and desist letter accusing them of trademark violation.

Undeterred, the 2600 group went on to register

VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com.

The point of this story is that it is impossible for a company to prevent someone from incorporating its name into a domain name in some way. Registering a few common misspellings (or using the UDRP to recover them if they have been registered by others in bad faith) makes some sense. But the DNS supports too many variations to make it possible to pre-empt criticism or capture all possible references to a company or product. Any attempt to protect massive “clouds” of names will be pointless unless draconian and undesirable restrictions are placed on the use of DNS.

All this assumes, of course, that the possession of these domain names is important and valuable. Here too, the case for a controlled vocabulary is based on highly questionable premises. As noted above, the idea that the majority of Internet users find their way around the Internet by typing in hundreds of different variations of domain names into their browser flies in the face of everything we know about user searching behavior. Contrary to Assumption #7, the registration of a domain name is no guarantee that a significant number of users will be attracted. Popular web sites that make money require expensive promotion, high-quality content, lots of links from other sites, and good word of mouth in the press and among users. What evidence we have suggests that simple, generic terms in the .com space do generate traffic, but there is also ample evidence that that type of random traffic by itself cannot sustain an online business.²¹

And users who type in the domain name of a company and finds something she did not expect to find – say, a protest site rather than the company – will not be smart

²¹ Cecily Barnes, “Catchy domain names lose their luster,” CNET News.com, October 16, 2000.

enough to look elsewhere. They will become completely diverted, and lost to the company forever. This notion is implausible on its face. It is like saying that someone who has incorrectly copied down a telephone number and dials the wrong person will not correct the error and redial.

11.5 Conclusion

To conclude, common pool conditions in the domain name space upset existing institutional methods of controlling how and by whom names can be used. This was true not just of trademark owners, but also of celebrities, political candidates, governments, and various organizations (mostly in Europe) supporting controlled appellations of origin. What started as a conservative reaction aimed at safeguarding older systems of control over names established by territorial institutions, however, has mutated into a radical program to create a new, global regime for the protection of property rights in names. WIPO, and to a lesser extent ICANN, believe that control of the root of the domain name system has created a historic opportunity to define and implement such a regime. Their object is to curtail the free adoption of names and transform domain names into a controlled vocabulary that gives a handful of privileged players – major trademark holders, international organizations, governments – sweeping rights over Internet identifiers.

This much is clear: the DNS protocol itself encourages and supports free expression. The protocol was designed merely to *coordinate* the assignment and resolution of multifarious name adoptions on the Internet. It was not structured to regulate their semantics, or to provide users with a clean and simple directory. The whole point of the protocol was to allow users to create their own semantics while ensuring that

the names remained unique. DNS's hierarchical delegation of authority allows the same label (e.g., *europe*) to show up in thousands if not millions of different places, under different top-level domains or second-level domains or third-level domains – or even on the right-hand side of a URL. Because responsibility is distributed down the levels of the hierarchy, there is room for vast amounts of variation in the policies and practices used to create naming conventions and assign names. Moreover, since the DNS name space is virtually inexhaustible, it gives users an extraordinary amount of flexibility to adopt whatever label they like. If the label they want within a specific domain is taken it is not that difficult to find a slight variation that isn't. As far as the DNS protocol is concerned, if the label is unique it is fine. It doesn't care whether the label is “confusingly similar” to a trademark or whether the person who adopted it has any authoritative connection to the referent. And the costs of entering a registration and propagating it throughout the Internet's intricate web of name servers are so low that anyone who can afford a PC and Internet access can probably afford to have their own domain name(s) as well.

To turn domain names into a controlled vocabulary is like pushing a heavy rock uphill. One must constantly work against nature. One must supplement the mechanical uniqueness enforced by DNS with exclusions, rules, and dispute resolution procedures to create what Jon Postel called a kind of “higher order uniqueness.” One must undermine or abolish the hierarchical structure of the DNS to account for subjective criteria. The UDRP, sunrise proposals, and name exclusions all deviate sharply from the original concepts and implementation of DNS in order to regulate the semantics of the space. In a fundamental sense, the ICANN-WIPO regime is at war with the DNS protocol itself, an attempt to turn domain names into something they are not.

