Technology for the Digital Lawyer III: Internet Infrastructure

[Tuesday, September 11, 2001]

READINGS

The Domain Names System

Domain names are, by now, ubiquitous -- having seized the media's great interest during the "dot-com" boom of the late 1990s. Yet relatively few people understand the technology behind domain names.

Part 1: Basic Information

We begin with the following good (though slightly dated) introduction:

Diane Cabell, Name Conflicts, Learning Cyberlaw in Cyberspace (1999).
[important: read Part I only]

A critical part of understanding domain names is visualizing the system that makes it work, and how the information travels. Consider a modified version of the graphic found in the Cabell reading:

![Diagram of Domain Name System]

Figure 1.

Also consider a graphic roughly illustrating how the DNS system works:
Try to determine how a computer in the PENN network would find the IP address information for www.mit.edu.

**Part 2: Growing TLD Space**

Since the Cabell document was written, a few technical developments have occurred. As a general matter, these developments can be characterized as gradually increasing and formalizing the TLD space. The first of these changes is not especially technical: a new (international) organization, called the Internet Corporation for Assigned Names and Numbers (ICANN) has taken over the "governance" of the domain name system. (Network Solutions, Inc. is still under contract to administer the root servers, but ICANN is at least officially in control. Second, ICANN has authorized the establishment of seven new TLDs. And third, more serious third-party, alternative domain names systems have cropped up - at least in part due to dissatisfaction with ICANN's performance. Consider the implications of each of these developments as you read the following:


[ you probably also want to click around the new.net site to get a feel for their plans ]

**About Web Servers and Pages**

Finally, it is also quite important to understand a few of the mechanics of how web pages are created, hosted, and displayed:

[read the linked web page only]

If you are interested in learning more about HTML, and perhaps dabling yourself, I suggest any of the several guides listed by Yahoo! (note that as a student at Penn you have web space on our server). But this is optional.
NOTES & QUESTIONS

1. Understanding the DNS. Consider for a moment the importance of the domain name system in the "popular" view of the Internet. Is this level of importance really warranted? Can you "exist" on the Internet without a domain name at all?

Assume that tomorrow the domain name system was turned off. (How would you do this?) Now think about what might happen, and what the response (other than turning it back on) would be. Does this thought exercise lend any insights into the appropriate understanding of the role of the DNS?

2. The Power of the Root. Yesterday we spent a great deal of time discussing the "decentralized" and "distributed" nature of the Internet. Yet those terms do not accurately describe the DNS. Does this create legal, business, or political implications? Can you reconcile the Internet with the DNS? What, really, is the extent to which the controller of the root DNS server has over the Internet? (And think again about where that server is, and who has the keys.)

3. Dueling Roots. The past six months has seen the first real challenge to ICANN's position as sole administrator of domain names. Looking again at Figures 1 and 2 above, consider how alternative DNS systems (like New.net) work. Also look again at the list of TLDs offered by New.net -- while at this point, there is no overlap with ICANN, this may change in the future. What then? If there is to be a single root, who gets to decide which one? Consider again how ICANN was granted authority, and whether this precedent is likely to continue.
Learning Cyberlaw in Cyberspace

NAME CONFLICTS Last updated on 25 August 1999

Diane Cabell, Fellow
Berkman Center for Internet & Society, Harvard Law School

Table of Contents

I. Technical Overview
Numbers Names Domain Name Management Root Server Alternative Roots Top Level Domains

II. DNS Administration
Privatization of Domain Administration Domain Registration Competition Uniform Global Dispute Resolution

III. Name Disputes
NSI Domain Dispute Policy Trademark Basics Case Law

INTRODUCTION

The practice of using domain names began as a helpful aid for routing data across the Net. During the gentle days of academic research, the simple policy of handing out a name to the first person that asked for it worked wonderfully well. When commerce hit the World Wide Web in 1992, trademark law came barreling right behind and the judicial debris continues to litter cyberspace. This module will describe how the domain name system actually works and who makes decisions about it, including dispute resolution policies. Trademark basics will be reviewed as well as important case law generated by the various uses of names on the Net.

Domain name disputes comprise the substantive area that is closest to being subjected to a uniform global regulatory mechanism. The hazards associated with such a new technical world order and the regulatory power embedded in code were once the province of esoteric academia. [Hear audio archive of Lawrence Lessig, New York New Media Association Panel, "The Internet & Public Policy: Who's in Control? " June 10, 1998.] As the general public begins to rely on the Internet as an important tool for commerce and communication, however, these issues are beginning to infect the mainstream consciousness.

I. TECHNICAL OVERVIEW

By now, everyone is familiar with the sight of a URL (Uniform Resource Locator), that combination of letters, slashes, dots, and numbers that makes up a web address (such as http://www.amazon.com). You know that if you type a URL into your browser, you will (usually) arrive at your desired destination as quickly as your Internet connection allows.

But how do you get there? Understanding the underlying technology and protocols of this everyday activity is essential to fully comprehending the legal issues at stake. We will use a fictional Harvard student as an example.

The Domain Name System (DNS) is the Internet equivalent of a telephone directory. It is the current method used to identify different computers so data packets may be properly routed across the Internet. There are two kinds of identifiers: numbers and names. Names are optional, but numbers are mandatory.
Each host computer on the Internet is assigned a unique identification number called an "Internet Protocol Address" (IP Address). An IP address is like a street address; it is the target for shipping data. Without an IP address, one is invisible in cyberspace. IANA, the Internet Assigned Numbers Authority (the administration of which is being transferred to the new private organization, the Internet Corporation for Assigned Names and Numbers, or ICANN) coordinates the assignment of numbers under contract to the US Department of Commerce. IANA begins by allocating blocks of numbers to Regional IP Registries known as RIRs (ARIN in North America, RIPE in Europe, and APNIC in the Asia/Pacific region). The RIRs then allocate blocks of numbers to large Internet service providers who in turn pass portions down to the smaller Internet service providers who share them with their users. Allocation is not entirely clerical. Although the task is mainly to avoid giving the same number to more than one host, there are issues having to do with keeping numbers within hierarchies so that routing tables (which direct traffic along each Internet node) remain as short and efficient as possible. While domain names may attract the world's attention, it is control over numbers that really determines access to the Net.

Harvard will assign our web-venturing student, whose name is "Fred," an IP address when he moves into the dorm. IP addresses currently consist of a numerical sequence (IPv4) that can contain as many as twelve numbers in 4 blocks (the segments of an IP address separated by dots "."). IPv4 consists of more than 4 billion addresses but that has already proven insufficient due to the inefficiencies of centrally managed IP address assignment processes. IPv6 has just been approved to expand the number base. Data packets, including e-mail, can be sent by simply using the IP address, e.g., Fred@208.218.131.20. Some domain names may be assigned a static (permanent) address while others are assigned dynamically.

Names

It is often reported that names were introduced in order to spare users the difficult burden of remembering long numbers. Indeed, http://www.harvard.edu is easier to remember than 128.103.200.101 but that is merely a side-benefit. The actual purpose is to permit greater efficiency when changes are introduced in the records associated with an individual identity (if the local network is reconfigured or the domain holder wishes to move to a different access provider, for example). Postel, J., Reynolds, J., Domain Requirements, 1984, RFC 920.

In the beginning, all traffic was routed to a single database listing all of the owners of host computers with their corresponding IP addresses (a host table). (Read about the history.) Identical copies of the list was copied by thousands of other servers for redundancy so that queries need not bottleneck at one central location—this served the distributive defense-oriented goal of making the Internet invulnerable to destruction. Entering all the new names to that single database and distributing fresh copies of the updated table became increasingly burdensome as the number of participants increased dramatically. Furthermore, the larger the list grew, the longer it took nameservers (computers loaded with name resolution software, such as BIND) to read through it to localize a particular address.

In the 1980s, strategic changes were implemented. Most importantly, the list was divided into hierarchical categories (domains) so that (a) each segment could be updated locally without having to revise the entire list (names no longer need to be globally unique, only unique within an organization as telephone numbers need only be unique within an area code, (b) maintenance of the data was distributed among the owners of the data instead of being assigned to a central administrator. Mockapetris, P., Domain Names - Concepts and Facilities, 1987, RFC 1034, Updated-by: Mockapetris, P., DNS Encoding of Network Names and Other Types, 1989, RFC 1101; Mockapetris, P. Domain names - Implementation and Specification, 1987; RFC 1035, Updated-by: RFC 1101 (above).

Domain Name Management

Domains (also called zones) are simply lists (also called registries); the domain name
hierarchy consists of lists within lists. Our student, Fred, has been registered by Harvard [registrar of the second-level domain (SLD) of "harvard"] and placed on its internal directory of names (its own zone file) and so he gets the address Fred@208.218.131.20, the (fictional) numerical equivalent of Fred@Fred_computer.fas.harvard.edu. When student "Fred" using the computer Fred.fas.harvard.edu wants to send mail to student "Mary" who uses the computer Mary.harvard.edu, he will type "mail mary@Mary.harvard.edu." His computer sends a message to the Harvard nameserver asking for the IP address of Mary.harvard.edu. The Harvard server sends it to Fred’s computer.

If Fred wants to send mail to student Joe using computer student23.mit.edu, Fred types "mail joe@student23.mit.edu." Fred's computer sends a message to Harvard’s nameserver asking for the IP address of student23.mit.edu. If Harvard’s nameserver has just been booted (meaning it has been recently restarted and has lost the copies of all the IP addresses that it already located) Harvard needs to ask the ultimate authority, a root server, for the IP address of ".edu." When Harvard receives the IP address of the .edu nameserver, Harvard then sends a message to .edu asking it for the number of mit.edu’s nameserver. When Harvard receives the address of MIT's nameserver, it sends a query to MIT asking for the IP address of student23.mit.edu. The IP address of student23.mit.edu (currently, Joe) is sent back in return.

Root nameservers have a database which lists the IP addresses of the nameservers for the top level domains (TLD) (.edu, .com, .net, .jp, .fr). The .edu nameservers have a database that lists the IP addresses of the second level domain (SLD) nameservers within the .edu top level domain (mit.edu, harvard.edu). Harvard's nameservers list the IP addresses of specific Harvard computers and any third level nameservers (e.g. fas.harvard.edu & cfa.harvard.edu). There can be any number of levels. Postel, J. Domain Name System Structure and Delegation, 1994, RFC 1591.

**Root Server**

The root server system is a set of around a dozen computers, each of which contains an identical copy of the same root file. One of them, [currently the "A" root server operated by NSI under contract to the United States government (USG)] contains the authoritative copy of the TLD zone file. The authoritative copy is the one that all others trust to be the authentic and contain the most complete and most current list of TLDs. The other root servers, which are owned an operated by several independent organizations, simply ask for a copy from A. Whoever manages the authoritative root may enter or delete TLDs. If .com were to be deleted from the root file, then the next time the other servers updated their copies, every single .com domain name would disappear from the Net. People and websites could still be reached using IP addresses, but it is highly likely that general havoc would reign.

Authority over the root file is another possible source of central control on the Internet. It could be used to dictate registration policy across all of the domains or even to regulate Internet content. The easiest way to keep traffic away from an "offensive" web site is to delete the name from the zone file and the easiest way to require zones to
police offensive sites is to threaten to delete the entire TLD. Lest one imagine that this power is unbridled, however, one must remember that the authoritative root gets it status only if the servers beneath it use it (that is, "point" to it) to get their directions. The TLD server owners may decide individually where to point, just as the owners of the root servers may decide individually what TLDs to include in their inventory. If the root is not being administered in a trustworthy fashion, or does not offer access to desirable domains, then the remaining root servers or the TLD servers can choose to reconfigure their machines to point to a different root.

There are competing (alternative) roots in existence now, but they are not widely used, either because of a lack of awareness, confidence, or interest or perhaps because the idea of a fragmented, unstable Internet is unwelcome.

Q. What are the boundaries between setting uniform standards and exercising monopoly power?

Alternative Roots

Alternative roots have been eyed warily by the Internet community because they lead to fragmentation of the Net. An alternative root is simply any other root file that does not receive its copy from the authoritative root administrator. Alternative roots have the capability of directing nameservers to TLDs that are not in the authoritative root database. If an independent techie, for example, wanted to set up her own top level domain (.foo, for example), she certainly is free to do so, after all, it's just a digital database. But how does traffic get routed to that TLD?

The decision to route traffic to one root or another is within the control of the user. When Fred establishes access through an ISP (Harvard acts as an ISP to students), and configures the settings, she enters the IP addresses for the nameservers that she wishes to use to locate information on the Net. Any user can choose any nameserver, including those that point to an alternate root, although most use whichever servers the ISP recommends. An alternative root may or may not include the authoritative root data as well as its own unique files. The current authoritative root, however, does not contain any alternative files. As multiple roots develop, there will be multiple networks, each a little different from the other and this is the kind of fragmentation can be seriously destabilizing. One cannot split a TLD among alternative roots, or else it sort of like reaching different companies when you call a phone number depending on which telephone you use.

Alternative roots have the potential of becoming filters of content. A government could easily build its own root containing only its preferred zones, and mandate its use. Pornography could be banished to an alternative root, or one could be devised as a safe haven for children.

In 1996, alternative networks received notoriety when hacker Eugene Kashpureff went beyond merely offering an alternative when he rerouted all web traffic headed to Network Solutions' InterNIC to his AlterNIC web site (which uses the gTLDs .sex and .med). He acknowledged doing this as a protest against NSI's monopoly in name registrations. Kashpureff fled to Canada, was extradited and pled guilty to wire fraud charges; he received a suspended sentence. (Read more about this: ZDNN Tech News Now, Internet Hacker Pleads Guilty, March 19, 1998.)

Q. Is competition at the root level better or worse for the consumer?

Q. Will alternative root administrators be liable under misappropriation or other theories by diverting traffic to competing zones?

Q. If you were responsible for thousands of domain names, how would you choose which root to use?

Top Level Domains

There are currently about 260 TLDs in the root zone file. About 250 of them are country code zones (ccTLDs) such as .us, .fr and .uk (United States, France, and the
The ccTLDs are run by local administrators in each country. Postel, J., IANA Policy on Delegated Domains, These administrators were originally experienced local technical personnel (usually academic) appointed by IANA but as the popularity and market value of domain registrations has increased, national governments are beginning to assert independent control over their ccTLD registries. Authority over individual ccTLD administration is therefore an evolving issue. Registrations in the .us domain are handled by a vast number of volunteers who are supervised by the Information Sciences Institute at USC under contract with NSI which is under contract with the US government. Cooper, A.; Postel, J., The US Domain, /RFC 1480./; The US Domain Registration Services.

There are also seven generic domains (gTLDs), operated by various entities under different restrictions. These domains were originally intended for uses categorized by function, such as .gov for government and .edu for education. The US government runs .gov and .mil. The gTLD .edu is limited to 4-year colleges and universities. The most populous gTLDs are .com, .org, and .net, operated by a private contractor, Network Solutions, Inc., (NSI). The distinctions among these last three categories have never been enforced and have become blurred over time. In mid-1999, almost 90% of all domain names registered worldwide had been registered through NSI. This market advantage got its impetus from the early search engines that only indexed these particular domains. It was furthered in 1992 when NSI was granted an exclusive government contract to operate in these domains as both a registrar (accepting applications for domain registrations from the public) and as a registry (entering that registration data into the TLD zone file). (Read the agreement.)

The registry of each TLD currently sets its own policies about name registration and dispute resolution. The technical parameters of name registration (how many characters it may contain, where the dots must appear, etc.) are the subject of protocols (determined by consensus of the engineering community). Beyond that, neither the government nor the technical administrators have heretofore attempted to impose any standards on registration policy; however, this is increasingly likely to change as use of the Internet accelerates.

Although ccTLDs were originally envisioned as being limited to domestic use, the registration policies of the various country code domains have evolved quite independently. Some still restrict themselves to local entities (Italy) but others sell registrations on the open market as if they were gTLDs (like the country of Tuvalu, which owns the coveted .tv domain). Some prohibit registration of product names or trademarks (Norway). Only a few (like Sweden) have a separate SLD for personal use.

II. DNS ADMINISTRATION

NSI ordinarily registers the first applicant to request any particular name, unless there is a complaint from the owner of a pre-existing national or federal trademark. Network Solutions’ Domain Dispute Policy, Revision 03, Effective February 25, 1998. NSI’s dispute policies have led to much trademark litigation, as will be discussed below in the section on Domain Name Disputes. While NSI remains a sole source government contractor, however, it enjoys immunity from anti-trust claims in the US, if not abroad. Tech Law Journal, Judge Rules in Domain Name Registration Suit, (April 10, 1998) and see collection of cases at The Perkins Coie Internet Case Digest, Antitrust. Elinor Mills, DOJ Renews Domain Name Registry Probe, Computerworld Online News, (May 6, 1999) (EU/UK anti-competition activity).

Privatization of Domain Administration

In 1996, as the growth of private and commercial use exploded, the Clinton administration recognized that the Internet was now such a broadly distributed network, with ownership of its constituent parts so widely scattered, that it was no longer appropriate for one single government to be coordinating its functions. There was also great dissatisfaction with NSI’s exclusive position in the most popular market. Following public hearings (including online sites for public comment), the government decided to withdraw from the role of technical coordinator and permit the private sector to assume this responsibility. US Department of Commerce White Paper,
In November 1998, the DOC entered into an agreement with ICANN giving the latter one year to develop methods and procedures for technical coordination in a manner that will ensure bottom-up coordination, market competition, global representation and stable operations. Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers (25 November 1998). Under that agreement, ICANN assumed the government’s oversight responsibilities for names, numbers, protocol parameters and the authoritative root and has since undertaken a series of steps to meet its MoU obligations.

http://www.icann.org/announcements.htm

Q. By inviting ICANN to assume responsibilities that were previously the responsibility of the Department of Commerce, is the USG transferring public assets or regulatory functions to a private entity?

Q. If so, under what authority does the USG transfer these responsibilities?

Q. How does a regulatory body assess the value of online public comment, given the absence of sender authentication?

Domain Registration Competition

There are two areas in which competition for domain registrations may exist: that of the registrar and that of the registry. The registrar collects a fee and data from the individual applying for a domain name. The registry charges a fee to the registrar to incorporate that data into the zone file. In many TLDs, the two functions are performed by the same entity.

In order to renew its exclusive contract as the com-org-net domain registry, NSI was recently required to admit competition at the registrar level. (Amendment 11) However, since NSI retains exclusive control of the zone files themselves, it remains at a competitive advantage over the other registrars both in terms of price (it charges the them $9 per registration to enter their data) and in terms of access (it enters its own clients’ data as well). Although five testbed registrars were approved by ICANN in April 1999, only two had begun operation by July. There are more than 50 approved registrars waiting for interoperability with NSI’s databases.

Registration with most TLDs is automated. (Example) The registration information is entered directly by the applicant on a registrar’s website and then automatically compiled in a backend database. Easy access to domain registration data is critical to the stable operation of the Internet. Much technical havoc can be generated that can only be resolved at the source, therefore it is necessary to know who actually operates the domain owner’s nameservers. Plaintiffs also want to know whom to serve in cases of web site malfeasance. This information has always been available through Whois, a searchable archive of every single domain name and IP address registrant in the com-org-net registries. Whois is also used to see whether a particular name is still available for registration. The Whois database, which is now an extremely valuable file, was established by NSI under its USG contract and NSI therefore has control over how much of the personal data is displayed on a Whois search. First Amendment activists want such data suppressed in order to protect anonymous speech. A. Michael Froomkin, Anonymity and Its Enmities, 1995 J. ONLINE L. art. 4. EU privacy rights may also conflict with public accessibility to some of the Whois data.

Q. What is the nature of a domain holder’s right in the domain registration? Is it a property right?

Q. Does NSI have a protectable right in the Whois database? Can blank space in a file be owned by anyone? If so, what is the nature of that right? If NSI doesn’t own the data, who does?

Q. What right does the USG have to the zone files under its contracts with NSI?

Q. Is there any need for a centrally managed registry if data from all registrars
Another level of competition is the registry level. One of the most eagerly awaited commercial decisions relative to the root file concerns the addition of new gTLD registries (.biz, .web and .shop are some of the proposals) that would be entirely independent of, fully competitive with, and possibly as lucrative as NSI's. NSI currently maintains the authoritative root file and must cooperate to open this gate, an action that appears to directly conflict with NSI's commercial interests.

Q. Is NSI obligated to make additions to the root file at the direction of the USG?

Q. How much can NSI cooperate in the process of admitting competing registrars without violating its obligation to its own shareholders?

There are many benefits to consumers that might result from the addition of more top level domains including longer and more secure registration periods and better prices. It would also ease the perceived shortage of names in cyberspace that exists because there are so many different users who share the same name in real space (such as MacDonald) but only room for one of them at "macdonalds.com". Unfortunately, there are also many complications. Unless these new extensions can add significant distinction to a name, they will simply offer more opportunities for trademark infringement. A further unresolved technical question is how to effect domain portability: if a domain holder cannot carry his own name with him from one registry to another, more competitive terms may be of little consequence.

Uniform Global Dispute Resolution

The Memorandum of Understanding with the USG directs ICANN to consider the question of adding more gTLDs. As part of that review, it is requested to take into consideration recommendations made by the World Intellectual Property Organization (WIPO) concerning: (i) the development of a uniform approach to resolving trademark/domain name disputes involving cyberpiracy; (ii) a process for protecting famous trademarks in the generic top level domains; (iii) the effects of adding new gTLDs and related dispute resolution procedures on trademark and intellectual property holders; and recommendations made by other independent organizations concerning trademark/domain name issues.

The Final Report of the WIPO Internet Domain Name Process, presented to ICANN in May 1999, proposes a uniform, mandatory domain name dispute policy (administered by WIPO) for all .com, .org and .net registrants. Final Report of the WIPO Internet Domain Name Process, WIPO Publication No. 92-805-0779-6 (April 30, 1999). Even some of its panel members have expressed concern over some of the recommendations. Prof. A. Michael Froomkin, A Commentary on WIPO’s The Management of Internet Names and Addresses: Intellectual Property Issues. If endorsed by ICANN, these procedures are expected to be imposed on domain holders by contract. ICANN took the WIPO recommendations under advisement and referred them to its Domain Name Supporting Organization, but also voted to require all new com-org-net registrars to adopt a uniform domain dispute policy although it left the choice of the terms of such a policy up to the agreement of the registrars themselves. ICANN Berlin Meeting Preliminary Report, Resolution on Report of World Intellectual Property Organization. Those that are currently operational have chosen to adopt NSI's policy. Register.com Dispute Policy.

Q. Is the WIPO uniform dispute policy a good solution to the cybersquatting/cyberpiracy problem? Is it a good solution to the domain name/trademark conflict?

Q. If the uniform policy only applies to gTLDs, will those registries be at a serious competitive disadvantage to the ccTLDs which are not bound by the policy?

Q. If the US and other nations pass individual anti-cybersquatting initiatives (see S.1255), how will this impact on any uniform policy directives from ICANN?
The Department of Commerce has given ICANN a one-year probationary period to establish a stable, competitive, representative, and bottom-up system of management for IP address allocation policy, root server oversight, and coordination of protocol parameter assignments. As a private, non-profit corporation established under California law, ICANN has been attacked as unrepresentative because its volunteer 9-member Interim Board was not publicly elected. In response to public criticism and government pressure, ICANN restructured itself to include an at-large membership (equivalent under California law to shareholders) that will elect half of its eventual 18-member Board. Internal and external review systems were also designed based on public input. What was once a lean, mean and very efficient technical administration is being rapidly layered with what some call "checks and balances" and others call "bureaucracy". To many Netizens, it looms as a new international regulatory body that will impose its will by a series of contracts of adhesion. Should there be centralized government in cyberspace? Lawrence Lessig, Reading the Constitution in Cyberspace, 45 Emory L. J. 869 (1996). See archives of the IFWP discussion forum which debates ICANN issues.

Unfortunately, ICANN has not developed a revenue stream at this time and remains an underdefended target of those who oppose any centralized oversight of the Internet. An effort to impose a domain registration fee was attacked in Congress as an unauthorized tax. Hear the audio archive of the July 199 House Commerce Committee hearing on "Domain Name System Privatization: Is ICANN Out of Control. With less than a year remaining to accomplish the task of centrally coordinating the vast multitude of conflicting interests which the Internet has generated, ICANN remains in a very fragile position.

III. NAME DISPUTES

Trademark conflicts have been the primary cause of most Internet litigation to date. This module will not cover disputes over general web site content, as those do not, outside of jurisdictional questions, raise questions that are unique to the Internet. This module will first consider disputes over the right to use a particular word in a domain address and then look at other unique hypertext applications such as links and metatags. Linking, tagging and framing may also present copyright issues. For a detailed discussion of the latter, see the module Copyright in Cyberspace.

There are two ways to resolve disputes between trademarks and domain names. One is through the dispute policy of the domain registrar; the other is through the courts. Each registrar may establish its own dispute policy.

Network Solutions' Domain Dispute Policy

There are more than 7,500,000 domains registered worldwide as of mid-May 1999. Over 60% (5 million) of them are in the .com registry. The TLDs .org and .net contain another million. (Domain Stats) NSI has a domain name dispute policy that is imposed by contract on registrants. Network Solutions Domain Dispute Policy, Revision 03 (effective 02/25/98). There are many contentious features of this policy, not least of which are the rights reserved by NSI (a) to modify the policy at any time (Sec. 5) and (b) to revoke, suspend, transfer or otherwise modify any registration at any time at its sole discretion (Sec. 7). See Oppedahl & Larson LLP, NSI Flawed Domain Name Policy information page for a review of litigation concerning NSI's dispute policy.

NSI's dispute procedures (Sec. 8 and 9) give preference to owners of national or federal (Principal Register only) trademarks over anyone who holds a domain with an identical name unless the domain was obtained before the effective date of the trademark registration. This is certainly the least expensive enforcement mechanism for those who actually have federal trademark registrations. The mark owner is simply required to send a letter of complaint to the domain holder and then send to NSI a copy of that complaint with evidence of delivery plus a copy of the trademark registration certificate. NSI will then contact the domain holder and ask for evidence of federal mark protection that predate the complaint. If none is provided, then NSI may opt to put the domain "on hold" (prohibiting anyone from using it), evict the domain holder or take any other action that it deems fit, such as transferring the domain registration to
the mark owner. If litigation is commenced by either party, NSI will maintain the registration status "as is", unless directed otherwise by a court of competent jurisdiction. Not all domain registrars are so compliant. Oggi Advertising Ltd v. McKenzie and others, CP.147/98 (High Court of New Zealand, Auckland Registry) 2 June 1998. See also Domainz Media Statement, 13 November 1998.

Q. Why not use a simple first-come, first-serve policy for registrations?

Q. Is there an inherent quality to a web address that gives trademark holders a perceived right to control use of their mark (or similarity) when used in one?

By ignoring design marks, common law marks and state registrations, NSI's policy provides no relief to most mark owners. Confusingly similar words and common misspellings, for example, are not addressed because the policy only applies to identical character strings. It offers no protection to fair use and disregards the privileges of non-commercial users. Diane Cabell, The InterNIK Dragon: A Fable for Cyberchildren, The Domain Name Handbook: High Stakes and Strategies in Cyberspace by Ellen Rony and Peter Rony, R&D Books, 1998. Nonetheless, like the proverbial magic bullet, NSI has passed through almost every attempt to hold it responsible for the resulting domain name confusion. Lockheed Martin Corp. v. Network Solutions Inc., 985 F. Supp. 949 (C.D. Cal. 11/17/97); Dan Goodin, Another Favorable Ruling for NSI, CNET News.com May 12, 1999.

Five new registrars have recently been admitted to compete with NSI to service the com-org-net domain complex. More than 15 more are waiting to come online. ICANN recommended that all of the com-net-org registrars adopt a uniform registration policy of their collective choosing. At present, they have adopted NSI's policy.

Where NSI's dispute policy is of no avail, parties have naturally turned to the courts, which have shown a great deal more respect for the existing principles of trademark law

Trademark Basics

What is the purpose of trademark protection? The Lanham Act, 15 U.S.C. §§ 1051 - 1127, was intended to make "actionable the deceptive and misleading use of marks" and "to protect persons engaged in . . . commerce against unfair competition." 15 U.S.C. § 1127. In essence, the purpose is to protect the consumer from waste and fraud. Important elements of trademarks are that 1) they must be distinctive 15 U.S.C. § 1052, 2) as long as there is distinctiveness, there can be multiple legitimate uses of the same mark, 3) rights in marks relate only to commercial activities and 4) if use is abandoned or if the use loses its distinctiveness, rights lapse.

A trademark is either a word, phrase, symbol or design, or combination of words, phrases, symbols or designs, which identifies and distinguishes the source of the goods or services of one party from those of others. 15 U.S.C. § 1127. A service mark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. Marks must be distinctive so the customer can tell which products are made by Sony from those made by General Electric.

Marks are generally classified in categories of increasing distinctiveness: (1) generic (describes the type of product itself, for example, "Ice Cream" ice cream); (2) descriptive (literally describes the product or its attributes such as "Cold & Creamy" ice cream); (3) suggestive (connotes qualities about the product without literally describing the qualities, such as "Blizzard" ice cream; (4) arbitrary (unexpected in the context of use, such as "Diesel" ice cream); or (5) fanciful (invoking imaginative images in the context of use, such as "Home Run" ice cream") and (6) coined terms (words that are made up purposefully to be used as a mark, such as "Zerious" ice cream). See Abercrombie & Fitch Co. v. Hunting World, Inc., 537 F. 2d 4, 9 (CA2 1976). The last four categories of marks are deemed inherently distinctive and are entitled to protection. In contrast, generic marks [those that "refer] to the genus of which the particular product is a species," Park' N Fly, Inc. v. Dollar Park and Fly, Inc., 469 U.S. 189, 194 (1985), citing Abercrombie & Fitch Co. v. Hunting World, Inc., 537 F. 2d 4, 9 (CA2 1976), supra] are not registerable as trademarks. Park' N Fly, supra, at 194.' For a more comprehensive discussion of these categories, see the
Abercrombie opinion. Personal names and surnames (Byrd’s ice cream) and geographic terms (Alaska ice cream) are not considered inherently descriptive. Despite these strictures, even generic and descriptive marks may get protection if they acquire "secondary meaning." This happens when the mark user takes the risk of building a brand identity in the absence of strong legal protection and does indeed establish a distinctive name in the mind of the consumer, such as Ben & Jerry’s Ice Cream.

Q. If the company CreditComm Services has acquired secondary meaning, will it have an action for infringement against credit.com?

There are two different ways to get trademark protection, either by actual use in commerce under common law or by registration under statute. In the US, the first to use the mark in commerce has priority of ownership and actual use is a condition for registration in most states. If one places the goods/services in interstate commerce (or intends to do so shortly), federal registration is available under the Lanham Act. USPTO (searchable database and online registration forms. In most foreign countries ownership belongs to the first to register the mark. The important point is that the same mark may be legitimately used by different owners in different jurisdictions. This multiplicity of commercial rights (not to mention non-commercial rights to use language for other purposes) conflicts with the DNS identification function which only admits one user to a particular character string.

Because the essence of a trademark is to identify the origin of a good, the owner of a mark must aggressively maintain its distinctiveness or else lose it through the principle of abandonment. The mark owner therefore has the right and obligation to prevent another from using the same or a confusingly similar mark on competing products. "Confusingly similar" is not an easy standard for a layman to follow. It includes foreign language translations of the mark, different words that nonetheless convey the same meaning, and variations in spelling.

To determine whether there is a likelihood of confusion, courts look at a number of factors including: (1) the degree of similarity between the marks in appearance and suggestion; (2) the similarity of products or services for which the name is used; (3) the area and manner of concurrent use; (4) the degree of care likely to be exercised by consumers; (5) the strength of the complainant’s mark; (6) actual confusion; and (7) an intent on the part of the alleged infringer to palm-off his products as those of another. Some courts add additional factors, such as whether the senior mark holder is likely to "bridge the gap" and start marketing its services or goods in the markets in which the junior user uses the mark. David Loundy, Primer on Trademarks.

Q. Should the Internet be considered a single area of use for assessing likelihood of confusion?

Q. If you believe that it should, how would you assess a conflict between tonyspizza.com (the website for a small pie place in Brooklyn), and Tony’s Pizza (a national chain of pizza makers)? How would the other factors bear on your assessment?

Q. If you believe that it should not, how do you respond to the assertion that the "area of use" factor was designed for the days when local businesses had no possible of conflicting with the branding of businesses in far-off locations and all that has changed with Internet use?

There is also an additional statutory protection for famous marks. "Anti-dilution" statutes exist in many state and national jurisdictions to prevent impairing the value of a famous or well-known trademark. [See,e.g., 15 U.S.C. 1125 ] The Federal Anti-dilution Act was specifically intended to apply to domain name. (See Loundy, supra, at fn 32) The Federal Trademark Dilution Act defines dilution 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." This statute provides for claims against non-competing and non-confusing uses, which have the effect of diminishing or diluting the effectiveness or distinctiveness of a mark. Under anti-dilution, the mark owner may prevent any new commercial use of the mark, regardless of the lack of competition or confusion if the new use blurs or tarnishes the
value of the famous mark by rendering it common place through overuse or by associating it with unsavory materials.

**Q.** What about generic marks that become famous, for example, Tide laundry detergent? Can it prevent new enterprises, such as a vendor of nautical maps, from using tide.com?

Unlike copyrights or patents, trademark rights can last indefinitely if the owner continues to use the mark to identify its goods or services. The term of a federal trademark registration is 10 years, with 10-year renewal terms.

The US Patent & Trademark office accepts domain names for registration as trademarks if the applicant offers services via the Internet. Further, specimens submitted in support of the application to show use of the mark must show use of the Internet domain name as a source identifier, not as a mere directional reference. In other words, it must be used to label the services, not simply as the equivalent of a telephone number or business address. Also, providing a service which is normally expected or routine in connection with the sale of one’s own goods is not a registerable service. By analogy with the registration of trade names, the more distinctive the presentation of the Internet domain name and the further it is physically removed from other informational data appearing on the specimen, the more likely the name will be perceived to function as a service mark. See the USPTO's Trademark Examination of Domain Names.

Closely related to trademark, and often of greater utility, are rights under principles of unfair competition/unfair trade practices and misappropriation which exist in most states under both common law and statute. Michelle L. Spaulding, The Doctrine of Misappropriation (1998).

Trademark and domain names are a poor fit. One admits many users to a particular space, the other admits only one. Some have suggested substituting a DNS taxonomy that inserts additional identifiers (e.g., united.airline.com and united.movers.com). Unfortunately there are multiple legitimate mark owners within such categories and many businesses whose product classification may not be intuitive. Just as important is the fact that Net users avoid long domain names.

**Case Law**

Courts have generally applied traditional trademark and unfair trade practice analysis to disputes involving domain names. See the module Jurisdiction over Cyber Actors for more detail.

**Jurisdiction & Liability**

Although there are some decisions to the contrary (see, e.g., Inset Systems Inc. v. Instruction Set, Inc., 937 F. Supp. 161, (D. Conn. April 17, 1996)), most US courts have held that passive websites that lack interactivity are insufficient to establish personal jurisdiction in a non-resident forum.

In Bensusan Restaurant Corp. v. King, 1996 WL 509716, 937 F. Supp. 295 (S.D.N.Y., Sept. 9, 1996), aff’d, 126 F.3d 25, 1997 U.S. App. LEXIS 23742 (2d Cir., Sept. 10, 1997), the court held that uploading a web site onto a server located outside the forum was insufficient, without more, to subject the webmasters to personal jurisdiction where the site clearly indicated that there was no intent to sell products to forum residents. This case involved a local music club that had the same name ("Blue Note") as a well-known New York jazz club. The web site included disclaimers of any association with the New Yorkers and only offered ticket sales by telephone within Missouri.


**Q.** Should the simple act of posting a web page (or registering a domain name) make one liable in any jurisdiction in which that page can be accessed? Consider
the fact that anyone posting a page knows that it is available to a worldwide audience.

If you believe that such liability should ensue, how would you recommend handling the following case: a US company registers “luftballoons.com,” a site devoted to selling and trading music by a largely-forgotten 1980s pop group. A German company, LuftBalloons, has a valid German trademark in the name and considers the US registration infringing. Does your answer change if you know that the German site has a huge following in Germany? What if the US company was aware of this?

If you believe liability should only attach in a limited jurisdiction, how would you set the jurisdictional boundaries?

Foreign courts have exercised jurisdiction without regard to site of the host server or the domain registry. Some of them have applied an "effects approach" which involved consideration of the location in which the plaintiff had suffered harm and held that it had jurisdiction. The reasoning is that since it could establish that a local resident could access the Web site in the jurisdiction and was misled or deceived. While these cases have so far involved a resident defendant, they may have broader consequence and permit US entities to be sued abroad for harm caused by a "US" site in foreign location and also for an American company to sue abroad in order to protect its trademark. Burk, Jurisdiction in a World Without Borders, 1 Va. J.L. & Tech. 3 (Spring 1997).

Squatters and Pirates

The most frequent basis for litigation involves the practices of cybersquatting and cyberpiracy. These terms have not been carefully defined and yet almost every court around the globe has universally condemned both practices, whether under trademark law or some version of unfair trade practices. See Diane Cabell, Foreign Domain Name Disputes (1998).

"Cybersquatting" generally refers to the practice of stockpiling domain registrations in bulk for future resale to the general public. This activity can be innocent of any extortionist intent as with entities that auction or resell domain registrations as a service to a general public intimidated by the technical complexity of the TLD registrar interface. "Cyberpiracy" on the other hand, refers in particular to the registration of well-known names with the intent of deriving revenue from the sale of another's branded property. It also includes the act of registering names that are confusingly similar to a famous mark or well-known name for the purpose of generating traffic to a web site that would be ignored but for the user’s confusion over the names. Examples of the latter include slight misspellings (nikee.com instead of Nike) or the use of different extensions (whitehouse.com is an adult sex site, whitehouse.gov is the page for the residence of the President). Drafting a consensus definition of cyberpiracy has been one of many hurdles in resolving domain disputes. See paragraphs 170 - 176, Final Report of the WIPO Internet Domain Name Process, WIPO Publication No. 92-805-0779-6 (April 30, 1999) at Courts have found both cybersquatting and cyberpiracy to be infringing practices.

A key issue has been whether registration of a domain alone (without any website activity) entails the necessary commercial use. Although many courts have claimed that mere registration alone does not constitute infringement, key early cases held that the registration in bulk coupled with an offer to sell provided the necessary commercial element to bring a successful claim of infringement against a cyberpirate. See Panavision International, L.P. v. Toepfen, 938 F. Supp. 616 (C.D. Cal. 1996), (denying motion to dismiss), partial summary judgment granted, 945 F. Supp. 1296 (1996) (against defendant Toepfen, partial summary judgment granted, 41 U.S.P.Q.2d (BNA) ¶ 1310 (Nov. 27, 1996) (for defendant Network Solutions, Inc.), summary judgment against defendant Toepfen aff’d, 141 F.3d 1316, 46 U.S.P.Q.2d (BNA) ¶ 1511 (9th Cir. Apr. 17, 1998).

While a geographical address may be required to refer to a location, and thus may be "generic" and not likely to be registerable as a trademark owned by a business at that address, this assumes that the business takes its mark from a fixed address. With Internet
addresses, the address is generally taken to match the business’ mark. Thus, "proximity" of the marks, i.e. the goods or services "labeled" with the mark, and how similar they are to each other is likely to be more important on the Internet than in the "real world." Dan L. Burk, Trademarks along the Infobahn: A First Look at the Emerging Law of Cybermarks 1 RICH. J.L. & TECH., Paragraph 62 (Apr. 10, 1995).

The case of Avery Dennison Corp. v. Sumpton, 999 F. Supp. 1337, 46 U.S.P.Q.2d 1852 (1998) involved a cybersquatter. Sumpton claimed to be running a domain registration service and had registered 12,000 common surnames for resale to potential clients for use as e-mail addresses. Two of those registrations were avery.com and dennison.com." These were found to be in violation of the Lanham Act’s anti-dilution protection of famous marks (15 U.S.C. 1125©) despite the fact that Avery Dennison was the owner of the domain "averydennison.com" and therefore in no way prevented from marketing under its actual trademark (which is limited to the combination of both words). The 9th Circuit reversed that decision largely on the grounds that Avery did not qualify as a "famous" mark under the anti-dilution standards. Avery Dennison Corp. v. Sumpton, Case No. 98-55810, August 23, 1999.

Q. Surnames are ordinarily not registerable as marks unless they acquire secondary meaning. Is trademark practice on the Net reversing the basic principles of this law?

Q. Read the Avery Dennison case and the statute in the above paragraph. In particular, pay attention to the following Avery passage and its surrounding text:

The court holds that for purposes of the Act, a famous mark is "used in the ordinary course of trade" when (a) it is registered as a domain name by a registrant who is not otherwise identified by or associated with any of the commonly accepted meanings of the domain name, and (b) it is not used by the registrant as its own domain name, but rather is held by the registrant for sale or license to others.

Under the reasoning of Avery, what justification would you offer for the ability of the domain name registrars, such as register.com, to conduct their business?

Mere registration of a domain may not give rise to any trademark rights in a name. According to the Ninth Circuit U.S. Court of Appeals, "Registration with Network Solutions...does not in itself constitute 'use' for purposes of acquiring trademark priority." Brookfield Communications, Inc. v. West Coast Entertainment Corp., ----, 1999 WL 232014, 50 U.S.P.Q.2d 1545 [9th Cir.(Cal.) Apr 22, 1999] (NO. 98-56918)

Non-commercial Use

Product Criticism

http://www.compupix.com/ballysucks is the URL for a site devoted to consumer complaints about Bally Total Fitness. District Judge Dean Pregerson reportedly refused to grant summary judgment to Bally on its claims that the site infringed on and diluted its registered mark. Additionally, the court reportedly invited the defendant to file his own summary judgment motion against Bally seeking dismissal of the claims against him. Bally Total Fitness Holding Corporation v. Andrew S. Faber, 29 F. Supp. 2d 1161 (C.D.Cal., Nov. 23, 1998). Other actions are pending in Arizona over a U-Hell website (U-Haul claiming trademark violation and libel) and in NY over http://www.chasemanhattansucks.com (under anti-dilution claims). See generally Andrew Marlatt, Update/Companies Take Complaint Sites to Court, Internet World (November 16, 1998).

Q. What about product information sites such as "furbyinfo.com" and "usedbeaniebabies.com" where the domain holder is legitimately reselling a product or providing other support to product purchasers?

Q. Those who post U.S.-based criticism web sites rely on the First Amendment to the U.S. Constitution to support their right to free speech. Do you think
Trademark owners have a right to insist that their trademark not be used in web site criticism? Should trademark law trump the First Amendment?

Q. If you believe that the trademark owners have a right to insist that their name not be used in this fashion, how do you reconcile this with the fact that U.S. companies are allowed to use a competitor’s trademarked name in advertising for purposes of product comparison?

**Free Speech**

Political use of domain names has not fared so well. In two different cases, protestors used the names of well-known organizations as domain names leading to sites filled with material in moral and political opposition to the goals of the organizations. In Planned Parenthood Federation of America, Inc. v. Richard Bucci, d/b/a Catholic Radio 42 U.S.P.Q.2d 1430 (S.D.N.Y. 1997), aff’d. - F. 3d - (2d Cir., Feb. 9, 1998), the court held that the defendant’s sales of books on the anti-abortion site was commercial use amounting to infringement. In Jews for Jesus v. Brodsky, 993 F. Supp. 282 (D.N.J., Mar. 6, 1998) there was even less commercial activity, so the court relied on the defendant’s avowed purpose of intentionally misleading consumers who thought they were reaching the actual organization.

Q. If there were no commercial activity at all, what claim, if any, could the plaintiffs have brought against the domain holder for attempting to divert traffic

**Reverse Hijackers**

There is growing concern on the Internet about the abuse of non-commercial domain holders, particularly because they rarely have the financial resources to protect themselves in court.

Cases that have roused particular ire among Netizens involved children with domain registrations using their personal names. Although the sites themselves were clearly non-commercial (detailing such events as school baseball games and camp activities), impatient trademark counsel nevertheless sent cease and desist letters which gave rise to the accusation of reverse domain hijacking. The term refers to the abuse of trademark rights that occurs when a mark owner threatens a non-commercial domain holder with litigation thereby forcing the holder to undertake the financial burden of defending a fair use. In both the Pokey and Veronica cases, a grassroots effort of Net activists and resulting negative media coverage resulted in the mark owners reversing direction. See Beth Lipton, Archie Comics Fights Parent for Domain, CNet News, (Jan. 15, 1999).

Q. What is the real cost of defending a non-commercial domain registration against a litigious trademark owner?

Some legal theorists believe that the Internet will necessitate reconsideration of the very nature of intellectual property rights. As more and more words are grabbed for proprietary use, we are running out of words (as well as artistic expressions, methods and processes) and into more frequent collisions with our Constitution. See the collection of essays written by Lawrence Lessig, Berkman Professor of Entrepreneurial Legal Studies at Harvard Law School.

**Commercial Use**

**Non-competing Use**

Using traditional trademark principles, a New York district court dismissed claims for trademark infringement, false designation of origin, state infringement and unfair competition brought by toy retailer Toys ‘R’ Us against a Massachusetts firearms dealer who operates out of his home and registered the domain name “gunsareus” for his Web site. Toys R Us, Inc. v. Feinberg, 26 F.Supp.2d 639 (S.D.N.Y., Oct 28, 1998).
The Court dismissed the claims in part because Richard Feinberg's domain name does not use the toy retailer's trademarked "R." The Court further emphasized that guns are quite different from toys and that Feinberg uses his Web site to sell his wares primarily to other firearms dealers whom the Court considered to be sophisticated consumers unlikely to be confused by the name "gunsareus."

Interstellar Starship Services, Ltd. v. Epix, Inc., 983 F.Supp. 1331, 1997 WL 736486, 45 U.S.P.Q.2d 1304 (D.Or. Nov 20, 1997) (NO. 97-107-FR) involved a defendant (Starship) that had registered and used the domain name epix.com to publicize a theater group performing the Rocky Horror Picture Show. Plaintiff, Epix, Inc., a circuit board and computer program manufacturer owns the federally registered trademark Epix. While the trademark was found to be valid, the court determined that the use by defendant did not infringe on the plaintiff's trademark because the required element of likelihood of confusion was missing. The court emphasizes that the relevant likelihood of confusion "is confusion that affects the purchasing decisions of actual or prospective purchasers of the products of Epix, Inc." There is another unusual element to this case. The two firms say the word "epix" differently ("ep-ix" versus "e-pics"). One of the sites has an audio script that pronounces the word to further distinguish it from the other.

Note that often a likelihood of confusion analysis includes not only confusion that would lead to a mistaken purchase, but also confusion that would lead a potential consumer to believe that the product sold is affiliated with the trademark owner.

**Competing Use**

A series of Playboy cases, Playboy Enterprises, Inc. v. Calvin Designer Label, 985 F. Supp. 1218 (N.D. Cal. 1997) (temporary restraining order) injunction granted, 985 F. Supp. 1220 (1997); Playboy Enterprises, Inc. v. Asiafocus Intern., Inc. , 1998 WL 724000 (E.D.Va., Apr 10, 1998) (NO. CIV.A. 97-734-A), have favored the trademark owner against use of the mark in the domain names (as well as in the website content and metatags) of competitors. These cases represent traditional trademark law applied in a traditional manner.

What if the competitor hasn’t yet begun to use the domain? One of the cases that has found liability for use of a mark in a domain name even in the absence of any product or service was Green Products, Inc. v. Independence Corn By-Products Co., 992 F.Supp. 1070 (N.D. Iowa, Sept. 25, 1997). The court directed defendant to transfer ownership of a domain name to the plaintiff owner of an identical trademark. The court found that defendant's conduct was likely to infringe plaintiff's mark, and to cause consumer confusion, even though, as of the date of suit, defendant had not operated a website at "greenproducts.com." The court rejected defendant's argument that its conduct would not confuse the public because defendant's site would prominently disclaim any relationship to plaintiff, and otherwise distinguish defendant's through comparative advertising. The court held that use of plaintiff's mark in a domain name would deceptively lure customers to defendant's site and thereby cause consumer confusion.

**Q. What claim could a trademark owner bring against someone who registers the same word but simply sits on it to prevent the mark owner from accessing it?**

One creative solution to conflict is an "intermediate home page" which involves the shared use of a domain name, either voluntarily or by stipulated judgment. Some are voluntary. See http://www.disc.com. Others have been court ordered as where two companies were found to be jointly entitled to the domain name. Mattel v. Hasbro (Mattel, Inc. et al v. Hasbro, Inc. et al., Civil Action No. 96-7635, (U.S.D.C. C.D. Cal.). An introductory page at http://www.scrabble.com/ allows the user to link to either "hasbrosnscrabble.com" or "mattelscrabble.com."

See the module Copyright in Cyberspace for a discussion of issues relating to the use of marks in the content of a web site such as links, frames and metatags.

**Q. Is the Internet a single market place for purposes of determining confusion?**
Anti-dilution/tarnishment

The fairly recent (1996) federal Anti-dilution Act, 15 U.S.C. 1125©, has special protections for famous marks and this is raising some of the most uncomfortable conflicts on the Net when it is used in an attempt to enforce US law beyond its territorial limits. The Act bans any new commercial use of a mark after it becomes famous, regardless of confusion, if the result is to diminish or tarnish the famous mark.
What:

ICANN is a non-profit, private-sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities. ICANN has been recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.

It is ICANN's objective to operate as an open, transparent, and consensus-based body that is broadly representative of the diverse stakeholder communities of the global Internet. With a small staff of 14, ICANN is funded through the many registries and registrars that comprise the global domain name and Internet addressing systems.

Who:

ICANN is a non-profit corporation with a 19-member volunteer Board of Directors. Its Board has worked to pave the way for a smooth and stable transition from the present technical management system, which has been funded by the US government, to a new privatized and internationalized system. The Board's chairman is Dr. Vinton Cerf, Vice President of Internet Architecture and Technology for WorldCom, widely regarded as one of the fathers of the Internet. The other Directors have been drawn from a set of specialized technical and policy advisory groups, and through open, worldwide online elections.

Together with its Board of Directors, ICANN builds consensus through three supporting organizations -- the Domain Name, Address, and Protocol Supporting Organizations -- which collectively represent a broad cross-section of the global Internet's business, technical, academic, non-commercial, and user communities.

Why:

In the past, many of the essential technical coordination functions of the Internet were handled on an ad hoc basis by U.S. government contractors and grantees, and a wide network of volunteers. This informal structure represented the spirit and culture of the research community in which the Internet was developed. However, the growing international and commercial importance of the Internet has necessitated the creation of a technical management and policy development body that is more formalized in structure, more transparent, more accountable, and more fully reflective of the diversity of the world's Internet communities. In a phased, co-operative process, ICANN has been assuming responsibility to coordinate the stable operation of the Internet in four key areas: the Domain Name System (DNS); the allocation of IP address space; the management of the root server system; and the coordination of protocol number assignment.

How:

As a technical coordinating body, ICANN's mandate is not to "run the Internet." Rather, it is to oversee the management of only those specific technical managerial and policy development tasks that require central coordination: the assignment of the Internet's unique name and number identifiers.

For More Information:

Andrew McLaughlin
Chief Policy Officer
ajm@icann.org
This page provides links to information about the introduction of new top-level domains (TLDs).

The .info, .biz, and .name TLDs are accepting registrations. Go to the InterNIC website for more information.

SEVEN NEW TLD PROPOSALS SELECTED FOR INTRODUCTION

At its meeting on 16 November 2000, the ICANN Board selected the seven new top-level domains (TLDs) listed in the chart below for negotiation of agreements allowing them to be included in the Internet's domain-name system. These are the first new TLDs (other than country-code TLDs) to be introduced to the Internet since 1988.

Before these TLDs become operational, the operator or sponsor of each of them must reach a contract with ICANN. The green shading in the chart below indicates that agreements have already been reached with .biz, .info, and .name.

<table>
<thead>
<tr>
<th>TLD</th>
<th>Sponsored/Unsponsored</th>
<th>Purpose</th>
<th>Applicant</th>
<th>Contact(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.aero</td>
<td>Sponsored</td>
<td>Air-transport industry</td>
<td>Societe Internationale de Telecommunications Aeronautiques SC, (SITA)</td>
<td>Rosa Delgado</td>
</tr>
<tr>
<td>.biz</td>
<td>Un-sponsored</td>
<td>Businesses</td>
<td>NeuLevel(then known as JVTeam, LLC )</td>
<td>Barbara Blackwell Manager, Public Relations Tel: +1 202 533 2730 Fax: +1 202 533 2976 http: <a href="http://www.nic.biz">www.nic.biz</a></td>
</tr>
<tr>
<td>.coop</td>
<td>Sponsored</td>
<td>Cooperatives</td>
<td>National Cooperative Business Association, (NCBA)</td>
<td>Paul Hazen</td>
</tr>
<tr>
<td>.info</td>
<td>Un-sponsored</td>
<td>Unrestricted use</td>
<td>Afilias, LLC</td>
<td>Roland LaPlante Afilias Ltd. 660 Newtown-Yardley Road Newtown, PA 18940 USA Tel: +1 215 504 4610 Fax: +1 215 504 1758 http: <a href="http://www.nic.info">www.nic.info</a></td>
</tr>
<tr>
<td>.name</td>
<td>Un-sponsored</td>
<td>For registration by individuals</td>
<td>Global Name Registry, LTD</td>
<td>Hakon Haugnes 125 High Holborn London WC1V 6QA United Kingdom tel: +44 207 025 2200 <a href="http://www.nic.name">http://www.nic.name</a></td>
</tr>
<tr>
<td>.pro</td>
<td>Un-sponsored</td>
<td>Accountants, lawyers, and physicians</td>
<td>RegistryPro, LTD</td>
<td>Elana Broitman</td>
</tr>
</tbody>
</table>

Recent announcements about the new TLDs:

- ICANN Accredits New Top-Level Domains -- .biz and .info Registration Process to Begin This Summer (15 May 2001)
DRAFTING OF REGISTRY AND SPONSORSHIP AGREEMENTS

In selecting the seven new top-level domains, the Board authorized the negotiation of TLD sponsorship and registry agreements with the sponsors and operators.

The selected TLD proposals are of two types. .biz, .info, .name, and .pro are intended to be relatively large, "unsponsored" TLDs. The other three proposals (.aero, .coop, and .museum) are for smaller "sponsored" TLDs. (Generally speaking, an "unsponsored" TLD operates under policies established by the global Internet community directly through the ICANN process, while a "sponsored" TLD is a specialized TLD that has a sponsor representing the narrower community that is most affected by the TLD. The sponsor thus carries out delegated policy-formulation responsibilities over many matters concerning the TLD.)

Negotiation of three of the agreements—.biz, .info, and .name—has been completed and registrations for those TLDs are already underway. Negotiations of the remaining TLD agreements, with .pro (unsponsored) and with .aero, .coop, and .museum (sponsored) are progressing.

A. .pro Agreement

Unsponsored TLDs such as the .pro proposal are operated under "Registry Agreements" with ICANN. A single form of agreement has been negotiated with all four new TLD operators, including .pro. It covers the common aspects of all four and it is hoped that this form of agreement will serve, perhaps with some minor modifications based on experience, as the agreement for unsponsored TLDs that may be introduced in the future. The single form of agreement refers to twenty-four appendices, many of which are customized to reflect special features of the four TLD proposals.

At its meeting in Melbourne on 13 March 2001, the ICANN Board adopted the following resolutions:

RESOLVED [01.24] that the President and General Counsel are authorized and requested to complete negotiation of the remaining unsponsored top-level domain appendices as soon as feasible and to post the resulting appendices on the ICANN web site, along with any minor corrections or adjustments to the base agreement and appendices as already posted;

RESOLVED [01.25] that the Board shall be notified of the complete posting of the agreement and appendices for any of the four unsponsored top-level domains (.biz, .info, .name, and .pro) and after that notification seven days shall be allowed for Board members to make any additional comments to the President and General Counsel;

RESOLVED [01.26] that in the absence of the request of any Board member to the contrary based on policy considerations, the President is authorized to sign the posted agreements after the conclusion of those seven days; and

RESOLVED [01.27] that upon signature of the agreements the President is authorized to take such actions, including causing reports to be made to the United States Department of Commerce, as appropriate to implement the agreements.

The table below lists the appendices for the .pro agreement that have been completed and provides links to them. The unlinked entries are not yet completed. As appendices are completed, they will be posted and linked from the table below. Recently revised documents are in italics.
### Unsponsored TLD Agreement

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>Format and Technical Requirements for Requests to Change TLD Nameservers</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Format and Technical Requirements for Requests to Change TLD Contact Information</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Functional Specifications</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Performance Specifications</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Service-Level Agreement</td>
</tr>
<tr>
<td>Appendix F</td>
<td>Registry-Registrar Agreement</td>
</tr>
<tr>
<td>Appendix G</td>
<td>Fees for Registry Services</td>
</tr>
<tr>
<td>Appendix H</td>
<td>Equivalent Access Certification</td>
</tr>
<tr>
<td>Appendix I</td>
<td>Registry Code of Conduct</td>
</tr>
<tr>
<td>Appendix J</td>
<td>Start-Up Plan</td>
</tr>
<tr>
<td>Appendix K</td>
<td>Names Reserved from Registration</td>
</tr>
<tr>
<td>Appendix L</td>
<td>Registration Restrictions</td>
</tr>
<tr>
<td>Appendix M</td>
<td>Enforcement of Registration Restrictions</td>
</tr>
<tr>
<td>Appendix N</td>
<td>TLD Zone-File Access Agreement</td>
</tr>
<tr>
<td>Appendix O</td>
<td>Whois Specification—Public Whois</td>
</tr>
<tr>
<td>Appendix P</td>
<td>Whois Data Specification—Independent Whois Provider</td>
</tr>
<tr>
<td>Appendix Q</td>
<td>Whois Data Specification—ICANN</td>
</tr>
<tr>
<td>Appendix R</td>
<td>Data Escrow Specification</td>
</tr>
<tr>
<td>Appendix S</td>
<td>Data Escrow Agreement</td>
</tr>
<tr>
<td>Appendix T</td>
<td>Monthly Registry Reports</td>
</tr>
<tr>
<td>Appendix U</td>
<td>Proof-of-Concept Reports</td>
</tr>
<tr>
<td>Appendix V</td>
<td>Initial Consensus Policies</td>
</tr>
<tr>
<td>Appendix W</td>
<td>Additional Covenants</td>
</tr>
<tr>
<td>Appendix X</td>
<td>Registry Operator's Domain Names</td>
</tr>
</tbody>
</table>

### B. Sponsored TLD Agreements (.aero, .coop, and .museum)

Negotiations for agreements with the sponsors of the three sponsored TLDs (.aero, .coop, and .museum) have been proceeding for some time.

As noted above, a **Sponsor** is an organization to which ICANN delegates some defined ongoing policy-formulation authority regarding the manner in which a particular sponsored TLD is operated. The sponsored TLD has a **Charter**, which defines the purpose for which the sponsored TLD has been created and
The Sponsor is responsible for developing policies on the delegated topics so that the TLD is operated for the benefit of a defined group of stakeholders, known as the Sponsored TLD Community, that are most directly interested in the operation of the TLD. The Sponsor also is responsible for selecting the registry operator and to varying degrees for establishing the roles played by registrars and their relationship with the registry operator. The Sponsor must exercise its delegated authority according to fairness standards and in a manner that is representative of the Sponsored TLD Community.

The extent to which policy-formulation responsibilities are appropriately delegated to a Sponsor depends upon the characteristics of the organization that may make such delegation appropriate. These characteristics may include the mechanisms the organization uses to formulate policies, its mission, its guarantees of independence from the registry operator and registrars, who will be permitted to participate in the Sponsor's policy-development efforts and in what way, and the Sponsor's degree and type of accountability to the Sponsored TLD Community.

In addition, the sponsored TLD must be operated in a manner that complies with ICANN-developed requirements concerning interoperability, availability of registration data, and the like intended to ensure that the interests of the overall Internet are served.

Negotiations for TLD Sponsorship Agreements have progressed to near-completion with MuseDoma, the Sponsor for .museum, and are also approaching completion with SITA, the Sponsor for .aero. In both cases, a base TLD Sponsorship Agreement has been completed. The TLD Sponsorship Agreement is intended as a model for use with other sponsored TLDs, and has 23 attachments allowing necessary customization for the different circumstances of particular Sponsors and sponsored TLDs. Negotiations have also been proceeding with the proposed Sponsor for .coop within this framework, but significant issues remain to be resolved.

The base agreement and attachments completed in the .museum and .aero negotiations can be viewed by clicking the links below.

<table>
<thead>
<tr>
<th>Attachment</th>
<th>.aero</th>
<th>.museum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment 1</td>
<td>.aero Charter</td>
<td>.museum Charter</td>
</tr>
<tr>
<td>Attachment 2</td>
<td>Delegated Authority</td>
<td>Delegated Authority</td>
</tr>
<tr>
<td>Attachment 3</td>
<td>Format and Technical Requirements for Requests to Change TLD Nameservers</td>
<td>Format and Technical Requirements for Requests to Change TLD Nameservers</td>
</tr>
<tr>
<td>Attachment 4</td>
<td>Format and Technical Requirements for Requests to Change TLD Contact Information</td>
<td>Format and Technical Requirements for Requests to Change TLD Contact Information</td>
</tr>
<tr>
<td>Attachment 5</td>
<td>Description of Sponsored TLD Community</td>
<td>Description of Sponsored TLD Community</td>
</tr>
<tr>
<td>Attachment 6</td>
<td>Minimum ICANN-Required Functional Specifications for Registry Services</td>
<td>Minimum ICANN-Required Functional Specifications for Registry Services</td>
</tr>
<tr>
<td>Attachment 7</td>
<td>Minimum ICANN-Required Performance Specifications for Registry Services</td>
<td>Minimum ICANN-Required Performance Specifications for Registry Services</td>
</tr>
<tr>
<td>Attachment 8</td>
<td>Start-Up Plan</td>
<td>Start-Up Plan</td>
</tr>
<tr>
<td>Attachment 9</td>
<td>Selection of Registrars</td>
<td>Selection of Registrars</td>
</tr>
<tr>
<td>Attachment 10</td>
<td>Minimum Commitments Required of Registered Name Holders</td>
<td>Minimum Commitments Required of Registered Name Holders</td>
</tr>
<tr>
<td>Attachment 11</td>
<td>Schedule of Reserved Names</td>
<td>Schedule of Reserved Names</td>
</tr>
<tr>
<td>Attachment 12</td>
<td>Challenges to Registrations in Violation of Charter</td>
<td>Challenges to Registrations in Violation of Charter</td>
</tr>
<tr>
<td>Attachment 13</td>
<td>Sponsor's Domain Names Registered Directly with Registry Operator</td>
<td>Sponsor's Domain Names Registered Directly with Registry Operator</td>
</tr>
<tr>
<td>Attachment 14</td>
<td>TLD Zone-File Access Agreement</td>
<td>TLD Zone-File Access Agreement</td>
</tr>
<tr>
<td>Attachment 15</td>
<td>Public Whois Specification</td>
<td>Public Whois Specification</td>
</tr>
<tr>
<td>Attachment 16</td>
<td>Whois Data Specification—Provider Access</td>
<td>Whois Data Specification—Provider Access</td>
</tr>
<tr>
<td>Attachment 17</td>
<td>Whois Data Specification—ICANN Access</td>
<td>Whois Data Specification—ICANN Access</td>
</tr>
<tr>
<td>Attachment 18</td>
<td>Data Escrow Format, Content, Schedule, and Procedure</td>
<td>Data Escrow Format, Content, Schedule, and Procedure</td>
</tr>
<tr>
<td>Attachment 19</td>
<td>Data Escrow Agreement</td>
<td>Data Escrow Agreement</td>
</tr>
<tr>
<td>Attachment 20</td>
<td>Sponsor's Monthly Reports</td>
<td>Sponsor's Monthly Reports</td>
</tr>
<tr>
<td>Attachment 21</td>
<td>Proof-of-Concept Reports</td>
<td>Proof-of-Concept Reports</td>
</tr>
<tr>
<td>Attachment 22</td>
<td>ICANN Baseline Policies</td>
<td>ICANN Baseline Policies</td>
</tr>
<tr>
<td>Attachment 23</td>
<td>Additional Covenants</td>
<td>Additional Covenants</td>
</tr>
</tbody>
</table>

**HISTORICAL MATERIALS**

Click here to see information we have collected from the application process.

Click here to see the topic paper on new TLDs from the Melbourne meeting.

---

Comments concerning the layout, construction and functionality of this site should be sent to webmaster@icann.org.

Page Updated 04-Sep-2001
(c) 2000-2001 The Internet Corporation for Assigned Names and Numbers All rights reserved.
New.net seeks to become the world's leading domain name registry by introducing and selling domain names with new extensions that offer greater relevance and meaning than current Web site addresses ending in .com, .net, and other existing top-level domains. We are making this possible initially by encouraging millions of users to activate their Internet browsers to recognize New.net domain names and partnering with leading Internet Service Providers to activate our domain names automatically at the network level. We now have tens of millions of users that have access to New.net domain names, and we are confident that New.net domain names will soon be recognized universally across the Internet. Our primary objectives are to sell domain names that individuals and companies genuinely want, and to make the Internet an easier place for users to find what they are looking for.

New.net was started in May 2000 by idealab!, a leading Internet incubator. We have developed proprietary technology that allows our domain-naming system to exist alongside the traditional naming systems currently in use on the Internet. New.net has applied for patent protection for this technology.

65,292,491 Internet users worldwide have access to New.net domain names*

© 2001 New.net, Inc. All rights reserved. Privacy Policy

* New.net domain names are accessible by persons that use one of our partner ISPs to access the Internet or who activate their browsers. This is limited now, but growing daily. For source information click here.
Serving Up Web Server Basics

By Chris Hughes and Gunther Birznieks

Contents

How a Web Server Works - Overview
What Is HTTP, and How Does It Work?
How Does a Web Server Serve Content?
How Do You Choose a Web Server Platform?
How Do You Organize Web Servers for Performance?
How Do You Configure Web Servers for Performance?
How Does Web Server Security Work?
How Does a Web Server Differ From an Application Server?
How Does a Web Server Run Web Applications?
Wrapping Up

How a Web Server Works - Overview

When discussing how a Web server works, it is not enough to simply outline a diagram of how low-level network packets go in and out of a Web server. To give such a nuts-and-bolts explanation some sort of practical value, it must be placed in context. Thus, this tutorial will discuss what a Web server does to enable a better understanding of how it does its work.

Years ago, when Web servers were first prototyped, they served simple HTML documents and images. Today, as we shall go into later in this tutorial, they are frequently used for much more.

The first step is to view the Web server as a black box and ask the questions: How does it work; What can it achieve? It's a safe assumption that most Internet
users believe a Web site's success or failure is due to its content and functionality rather than the server used to power it. However, the choice of the correct server, and understanding its capabilities and limitations is an important step on the road to success.

So what does a Web server do? As we mentioned earlier, it serves static content to a Web browser at a basic level. This means that the Web server receives a request for a Web page such as


and maps that Uniform Resource Locator (URL) to a local file on the host server.

In this case, the file

index.html

is somewhere on the host file system. The server then loads this file from disk and serves it out across the network to the user's Web browser. This entire exchange is mediated by the browser and server talking to each other using Hypertext Transfer Protocol (HTTP). This workflow is shown in the figure below.

![Diagram of Web Server Workflow]

That's all there is to it.

But if it's that simple, then why such an in-depth tutorial?

Because this simple arrangement, which allows the serving of static content such as HyperText Markup Language (HTML) and image files to a Web browser was the initial concept behind what we now call the World Wide Web. The beauty of its simplicity is that it has led to much more complex information exchanges being possible between browsers and Web servers.

Perhaps the most important expansion on this was the concept of dynamic content (i.e., Web pages created in response to a user's input, whether directly or indirectly). The oldest and most used standard for doing this is Common Gateway Interface (CGI). This is a pretty meaningless name, but it basically defines how a Web server should run programs locally and transmit their output through the Web server to the user's Web
browser that is requesting the dynamic content.

For all intents and purposes the user’s Web browser never really has to know that the content is dynamic because CGI is basically a Web server extension protocol. The figure below shows what happens when a browser requests a page dynamically generated from a CGI program.

The second important advance, and the one that makes e-commerce possible, was the introduction of **HyperText Transmission Protocol, Secure (HTTPS)**. This protocol allows secure communication to go on between the browser and Web server.

In a nutshell, this means that it is safe for user and server to transmit sensitive data to each another across what might be considered an insecure network. What happens when the data arrives at either end is another matter, however, and should not be ignored. We will discuss this a bit later.

The simplicity of the above arrangements is deceptive, and underestimating its complexities often leads to bad decisions being made about the design of a Web-hosting infrastructure. It is too easy to focus on the design of the Web pages themselves and the technologies used to create dynamic content, such as Java, Javascript, Perl, C/C++, and ASP, and to subsequently miss the fact that each of these technologies can be aided, or hindered, by the platform on which they are to be run -- the Web server itself.

In other words, explaining how a Web server works involves discussing more than just how a Web server serves documents. We will go over the following topics in our quest to finding out what and how a modern Web server goes about doing its activities.

- What Is HTTP, and How Does It Work?
- How Does a Web Server Serve Content?
- How Does a Web Server Accept Connections?
- How Do You Choose a Web Server Platform?
- How Do You Organize Web Servers for Performance?
- How Do You Configure Web Servers for
Performance?
- How Does Web Server Security Work?
- How Does a Web Server Differ From an Application Server?
- How Does a Web Server Run Web Applications?

We will start by explaining the low-level details the underlie what a Web server must do. Then, we will discuss the issues surrounding the use of a Web server and how it fits within the scope of other infrastructural elements of the Internet. We will then close with a discussion of the relationship that applications have with Web servers.

Next: What’s HTTP?