

## TECHNOLOGY AND INSTITUTIONAL INNOVATION: INTERNET DOMAIN NAMES

by

Milton Mueller \*

### A. Introduction

This paper examines the property rights conflicts over Internet domain names that emerged as the Internet was commercialized and privatized. The events are interesting because they are exemplars of institutional innovation on an international scale catalyzed by technological change. The study draws on concepts of institutional change developed by North [1990, 1993] and empirical literature on the economics of property rights (e.g., OSTROM [1990]; LIBECAP [1989]). The general framework of the new institutionalist economics (NIE) is used to organize and illuminate a narrative about how the commercialization of Internet domain names led to the formation of a new international regime for regulation and dispute resolution. The empirical evidence derived from the narrative is in turn used to gain a critical perspective on the theory.

In this case, the driver of institutional innovation is technology's ability to create new forms of value. Innovation emerges out of conflicts in the definition or establishment of property rights in a new resource. As a counterpoint to the gradual and incremental model of change emphasized by the NIE, the example of the Internet argues that technology's ability to create new resources can serve as the catalyst of fairly rapid and disruptive institutional change. It also corroborates LIBECAP'S [1989] findings about how profoundly the path of institutional change is affected by conflicts over the distributional issues inherent in the definition of property rights.

The first section discusses the NIE literature on institutional change and its treatment of technology. Section 2 outlines a conceptual framework that attempts to identify the conditions under which technological change leads to institutional innovation. Section 3 provides some background information about domain names as economic and technical resources. The fourth section applies the conceptual model developed in Section 2 to a historical narrative of Internet governance.

---

\* Milton L. Mueller is Associate Professor, Syracuse University School of Information Studies, Director of Graduate Program in Telecommunications and Network Management, and Senior Associate of the Global Affairs Institute, Maxwell School of Public Administration.

## **B. Technology and the NIE Theory of Institutional Change**

The new institutional economics (NIE) is closely linked to and in many ways conceptually dependent upon the economic analysis of property rights and transaction costs (COASE [1937, 1960]; DEMSETZ [1964, 1966, 1967]; ALCHIAN [1965]; FURUBOTN AND RICHTER, [1998]). However, as North [1993, 36] observes, although the early property rights literature examined the efficiency implications of different property arrangements, it tended to treat their formation and evolution as exogenous factors. It was an ambitious attempt to endogenize institutions using a framework compatible with the basic assumptions of neoclassical economics that formed the basis of North's theory of institutional change.

NORTH [1990, ch.1] defines institutions as the rules, both formal and informal, that constrain human action. Institutions channel human behavior into certain paths by affecting relative transaction costs; i.e., by making some kinds of interactions highly costly and uncertain while making others convenient and secure.

In North's theory, the drivers of institutional change are the "opportunities perceived by entrepreneurs" who are decision-makers within organizations. Opportunities can be created by external or internal factors; i.e., by changes in relative prices (external) or by (internal) "changes in perception of relative costs caused by the acquisition of skills and knowledge or by changes in taste." [1991, 37] North summarizes his theory of institutional change as follows: "Institutions, together with the standard constraints of economic theory, determine the opportunities within a society. Organizations are created to take advantage of those opportunities, and, as organizations evolve, they alter the institutions. The resultant path of institutional change is shaped by (1) the lock-in that comes from the symbiotic relationship between institutions and the organizations that have evolved as a consequence of the incentive structure provided by those institutions and (2) the feedback process by which human beings perceive and react to changes in the opportunity set" (NORTH [1990, 6]).

North's definition of the sources of institutional change does not seem to provide for a sharp, qualitative distinction between equilibrium and disequilibrium in institutions. Changes in relative prices, in taste, and in learning occur at every moment in a complex, dynamic society. Thus, in North's view institutional change is overwhelmingly gradual and incremental, and within his model it is difficult to distinguish "institutional change" from the historical process in general.

Contemporaries of North offer less sweeping, more empirical attempts to explain institutional differences. Libecap [1989] and Ostrom [1990] focus on the transition from common pool resources to private property or collectively regulated regimes. LIBECAP [1989] provides considerable insight into the conditions that produce different institutional outcomes. He notes that different property rights arrangements will not only have varying production effects, but will also produce winners and losers in the distribution of wealth. In his analysis, political bargaining over these distributional issues is the chief determinant of why there is such variety in institutions, and why they can settle upon and maintain economically inefficient forms for a long time [1989, 7]. Libecap identifies five factors that will influence the outcome of

distributional bargaining: i) the size of the expected gains from institutional change; ii) the number of bargaining parties; iii) the heterogeneity of the bargaining parties; iv) the skewness of the current and proposed share distribution; and v) information problems. [1989, 11]

Unlike the “old” institutional economics, the NIE theory does not afford any special attention to the role of technology in institutional change. (RUTHERFORD [1994, 180] notes that the older institutionalist literature “contains many suggestive ideas on...the unintended impact on institutions of intentionally introduced alterations to the technical and material means through which individuals make their living.” See BUSH [1987] for an overview.) In North’s framework, technological change is mentioned only in passing, and is reduced to one of several methods of changing relative prices [1990, 84]. Similarly, LIBECAP notes briefly that technology can “reduce the costs of production or of defining and enforcing property rights.” (1989, 9) In FUROBOTN AND RICHTER’S [1998] thorough and estimable overview of NIE, the word “technology” does not even appear in the index.

It is evident from the references above that when North and Libecap refer to technological change they mean incremental changes in technique that make more efficient use of *existing* resources, improve *existing* production processes, or reduce the costs of defining and enforcing *existing* property rights. Missing from this picture is an explicit recognition of technology’s ability to create *new* resources – and with it, new forms of property. This kind of change is highly significant for an analysis of institutional change, because it can disrupt an existing institutional order and lead to a new equilibrium.

### C. Technology and Institutional Change

Below, I develop an analysis of the way new technological systems can trigger institutional innovation. This is conceived not as a departure from the NIE model of institutional change, but as an elaboration of it – the focus is still on changes in transaction costs and the bargaining over the distribution of benefits attendant upon the initial definition of property rights. No effort is made to argue for the generality of the framework. It is simply used to illuminate a particular historical case, and thus serves as an existence proof of technology’s ability to trigger institutional innovation.

I identify a three-stage process of change:

1) The development of a technical system begins to vest a new resource with substantial economic value. I call this process *endowment*. A new technology can suddenly invest resources or relations with great value, imposing upon society the need to define new rules that regulate access to it. Property rights must be specified in a novel context. The commercialization of broadcasting in the early 1920s is an easily understood example of this phenomenon. Broadcasting suddenly endowed certain parts of the electromagnetic spectrum with great economic and political value, triggering monumental political and legal struggles over its control (HAZLETT [1990], MINASIAN [1970]). The problem was not simply one of coping with the land rush created by the sudden opening of an unoccupied frontier, but one of defining, assigning, and allocating rights to a new kind of resource, the behavior of which was not well understood.

The initial encounter with this problem in the mid-1920s left in place an institutional regime of public trustee licensing that stayed in place for seven decades, and had profound impact on public communication in America.

2) Endowment creates a new *arena of appropriation*, a site of collective action in which actors attempt to establish property rights in the new resource so that they can benefit securely from its economic and political value. The formation of an arena of appropriation around a technologically endowed resource bears some similarities to the transition from a common pool resource to a private property regime. Both involve an appropriation process and potential conflicts over distributional issues. Both involve some uncertainty about technical issues involved in the definition of rights (e.g., dealing with externalities when enclosing common fields, water rights, etc). However, because common pool resources typically have been exploited for many years before they undergo such transitions, the uncertainties surrounding rights definition are probably less than in technological endowment. Likewise, the opportunities for first-mover advantages in technological endowment are probably greater.

3) Institutional innovation occurs when, during the appropriation process, two distinct types of property rights problems arise:

- a. There is a bootstrapping problem. Economic agents competing for access to the new resource are faced with substantial uncertainties about who among existing organizations has legitimate authority to establish, recognize, or enforce property rights. There may also be uncertainty about how to define rights (Libecap's "information problems"). These problems become especially interesting in an international context, where there is no single sovereign authority.
- b. There is conflict over the distribution of transaction costs, a conflict in which the economic stakes are high. Actors may propose novel institutional frameworks in order to capitalize on a unique opportunity to engage in large-scale shifts in the distribution of transaction costs.

The bootstrapping problem leads to institutional change because it tests the legitimacy of existing arrangements and creates entrepreneurial opportunities for organizations to assert a new kind of authority. Such assertions of authority or attempts to fill a perceived power vacuum may disrupt important aspects of the old order.

A new arena also creates unprecedented opportunities for large-scale *transaction cost shifting*. Depending on how property rights are defined, transaction costs may be dramatically reduced for some actors and increased for others. As appropriation occurs, there will be political and legal conflict over the distribution of costs and benefits. By proposing and winning acceptance of novel institutional arrangements, a coalition of organizations may engineer into place a highly favorable distribution of transaction costs that can last for a long period of time.

The paragraphs above sketch in general terms the conceptual scheme I will apply to the domain name controversy. Before applying that framework, however, some descriptive material about the underlying technology of domain names and the Internet is required.

## I. The Technology of Internet Domain Names

What we refer to as "the Internet" is really just the use of a common protocol suite and a common naming and addressing space to interconnect millions of autonomously administered computers and networks. The Internet's simple, open platform freed data communication from variations in hardware and software and allowed applications and information content to be controlled by end users rather than central network administrators.

The Internet is not, however, the completely decentralized and uncontrollable system it is sometimes made out to be. Critical to its functioning is a standardized, coordinated addressing scheme. The Internet relies on two distinct forms of addressing. One, known as the "domain name system" (DNS), consists of hierarchical strings of alphanumeric characters that usually form recognizable words or phrases to users. (The top of the hierarchy is at the right-hand side of the name.) Domain names are visible in email addresses (e.g., username@yale.edu) and in Web URLs (e.g., www.company-name.com). The other form of addressing, known as Internet Protocol (IP) addresses, are 32 bit numbers, and are assigned either statically or dynamically to particular computers. IP addresses are the ones that are actually used by machines to address and route data packets.

Domain names are used because they are easier to remember and key in than numbers and because they provide a more permanent identifier than IP addresses, which network administrators may need to share or rearrange. Domain names serve as a more persistent and human-friendly identifier. The use of domain names as a mask for IP addresses, however, makes it necessary to maintain databases on the network capable of matching a domain name to its associated IP address. That process is known as domain name *resolution* and is performed by *name servers*. In essence, the DNS is a globally distributed, hierarchically organized database that tells computers where they can match the domain name of the computer they want to communicate with to the appropriate numerical IP address. It is also a distributed, hierarchically organized method of assigning unique names.

Domain names and IP addresses are exclusive resources, and each introduces an element of centralization to the Internet's operation. Each name and address must be unique or else data will be misdirected. Name and address assignment on a large, rapidly growing network such as the Internet poses a major coordination problem. It may also pose a resource allocation problem, as the supply of addresses may be depleted or users may compete for desirable names. Generally, some form of centralized administration or coordination is required to ensure the uniqueness of address or name assignments. When contention for resources occurs, some rationing principle must be employed. Until recently, the centralized functions were performed by the US government, or by private contractors acting under its direction. The commercialization and globalization of the Internet, however, initiated a debate over privatizing and distributing internationally the responsibility for coordinating name and address assignment. It also initiated intense economic conflicts about the principles governing the assignment of domain names.

The DNS reduces the complexity of coordinating unique address assignments by delegating responsibility for name assignment and resolution in a hierarchical fashion (SU AND

POSTEL [1982] MOCKAPETRIS [1987]). At the top of the hierarchy there is an unnamed “root” that stores an authoritative list of top-level domain names (TLDs). For each TLD, the root directory provides pointers to name servers that contain authoritative lists of second-level domain names registered under that TLD. These lists are called “zone files.” Within each zone file, there is a pointer to name servers that know where to resolve second-level domain (SLD) names registered, and so on down the hierarchy.

A unique domain name can be recognized and function as an address because of the existence of a coordinated, authoritative root at the top of the hierarchy. Currently, there are 12 root servers distributed around the world, but they all “slaves” that take their data about the composition of the top-level from a single, “master” known as the “A” root server. The authoritative root assures that there are no conflicting name assignments and that every computer in the world knows where to find any other computer. The authoritative nature of the top of the hierarchy, however, also has made it a point of centralized policy control.

Currently, there are only 250 top-level domain (TLD) names in the root servers. 243 of these are two-letter country codes, most of which are based on the ISO-3166-1 standard.<sup>1</sup> There are also seven three-letter suffixes (Table 1) that represent a rudimentary taxonomy of the type of organizations that might use Internet domain names.<sup>2</sup> The former are often referred to as country code TLDs (ccTLDs) and the latter are called generic TLDs (gTLDs). As of late 1999, over 74 percent of the world’s domain name registrations are under the gTLDs .com, .net, and .org; sixty percent are under .com alone.

| Top-level domain name                   | Intended registrant type                      |
|---|---|
| .com                                    | Commercial                                    |
| .org                                    | Catch-all, non-profit and “other”             |
| .net                                    | Internet infrastructure providers             |
| .mil                                    | U.S. military                                 |
| .edu                                    | Four-year higher education institutions       |
| .int                                    | International treaty organizations            |
| .gov                                    | U.S. government                               |
| Country codes: .uk, .de, .jp, .my, etc. | Determined by national registration authority |

**Table 1: Top-Level Domain Names**

1 The International Standards Organization ISO-3166-1 list is a list of two-letter codes for “countries” maintained by a UN agency in Berlin.

2 As domain name registration has become more commercialized, the categorical distinction between registrations in the com, net and org TLDs has broken down. All three are considered “open” gTLDs.

The number of generic top-level domains has been frozen into place for four years. These restrictions on the number of TLD names are entirely *administrative*. Technically, the DNS could accommodate thousands, if not millions, of new TLD names.<sup>3</sup> Also, there is no technical reason to restrict the number of characters in the TLDs to two or three; TLDs could spell complete words just as SLDs do (although for efficiency and usability reasons it makes sense to limit the number of characters as much as possible). Thus, it follows that the parameters of the Internet domain name space can respond to forces of supply and demand.

## II. Application of the Model to Internet History

This section combines a narrative history of Internet domain name policy with the model of technology-induced institutional change outlined above. The argument proceeds in five steps.

First, the commercialization and growth of the Internet created a new resource with substantial value. The resource in question was the domain name space, especially its root directory, which provided the basis for global connectivity among computer networks.

Second, in the course of endowing that resource with value, the growth of the Internet created a new arena of appropriation. The problem of deciding who “owned” the root, when and how TLDs could be added to it, and the nature of property rights in individual domain names and the zone files of a top-level domain became contentious and economically significant.

Third, the process of appropriation faced serious bootstrapping problems. Authority over the root was unclear and the efforts of various domestic and international organizations to assert control over it suffered from attacks on their legal, political, and ethical legitimacy.

Fourth, there was a major conflict over the distribution of transaction costs between trademark owners (a well-organized, powerful interest group), domain name registration businesses and domain name registrants.

Finally, institutional innovations emerged in response to these problems. The discussion focuses on the formation of a new international non-profit corporation, the Internet Corporation for Assigned Names and Numbers (ICANN), and on a new system of global dispute resolution proposed by the World Intellectual Property Organization (WIPO) and implemented by ICANN.

### 1. Endowment

The Internet domain name system was used for about twelve years (1982-94) without creating any significant public policy issues. During those years, the Internet was mostly closed to the general public and to commercial uses and applications. As a research and education

---

3 The configuration of the NSI root server as of December 1998 put all TLDs in the same file as the second-level domain names in the dot com TLD. The dot com TLD contained over a million names, indicating that the root could have handled that many TLDs.

network subsidized by the US military and later by the US National Science Foundation (NSF), the Internet was relatively small in scope and insulated from commercial forces. Among other restrictions, NSF imposed an “acceptable use policy” (AUP) in 1985 that prohibited commercial traffic on the subsidized Internet backbone. Government agencies or contractors handled the central coordinating functions. Thus, during that period name and address assignment was an administrative task performed via contractual terms with the government, not an institutional problem that required the development of public laws or regulations. In July 1991 only 645 second-level domain names had been registered, and more than half of them were under the .edu, .mil, and .gov TLDs.

In 1992 the NSF began to privatize the telecommunications infrastructure of the Internet. It gradually withdrew subsidies from Internet backbone and access providers and permitted the growth of a private, commercial Internet Service Provider (ISP) industry. In 1995 it shut down the NSFNet backbone and its function was seamlessly taken over by private telecommunication firms. With the closure of the subsidized backbone the AUP restrictions disappeared.

The year 1995 can be used as the date when the Internet became a truly commercial, public medium, as the popularization of the World Wide Web application facilitated the explosion of consumer and business interest in the Internet.<sup>4</sup> The rapid growth of users produced a rush of demand for web sites, and every new business with a web site needed a domain name. The number of new registrations went from 300 per month in 1992 to 45,000 per month by late 1995. From 1995 to 1996 the number of registered domains increased from 150,000 to 637,000, with .com alone accounting for 60 percent of them. The non-commercial TLDs .edu, .mil, and .gov now constituted only 2 percent of total registrations.

Opening the Internet to commercial use played a key role in “tipping” an ongoing competition between incompatible data communication standards towards convergence on the Internet’s TCP/IP protocol. The network externalities associated with the growing dominance of TCP/IP in data communications amplified the value vested in the Internet root and the top level of its naming hierarchy. Very quickly, the root of the Internet became the nexus for the interconnection of computers everywhere in the world.

The growing importance of the Internet was soon reflected in the value attributed to domain names and the domain name registration business. Before 1995, in keeping with the non-commercial origins of the Internet, domain name registrations were distributed on a first-come, first-served basis to authorized parties for free. Accepting registrations and storing them in a database was a job performed by US government contractors, the costs borne by US taxpayers. Once the Internet’s commercial potential was discovered, however, the exploding scale of registration made the original contract unremunerative; moreover, it no longer made sense to subsidize the process. In 1995 the US government allowed Network Solutions Inc. (NSI), the contractor responsible for registering domain names in the gTLDs .com, .net, and

---

4 The first widely disseminated Web browser, “Mosaic,” was produced by the University of Illinois NCSA beginning in 1993. In 1994 the commercialized version of Mosaic known as Netscape was released.

.org, to charge \$50/year for domain name registrations. Outside the USA, many registration authorities running ccTLDs had already begun to charge annual fees for registrations. Domain name registration in the InterNIC's generic TLDs quickly evolved into a multi-million dollar business. NSI's exclusive right to administer those TLDs was no longer just a government contract; it was a grant of an exclusive monopoly on a lucrative market.

Commercialization transformed the nature of domain names as much as the business of registering them. Domain names before had been nothing more than user-friendly addresses. In a commercial marketplace, however, they came to be seen as marketing tools and brand names, the catchier and more advertisable the better. Names registered under .com in particular began to acquire a premium value. As the only explicitly commercial generic TLD, many consumers began to assume that an organization or business they wanted to find could be located by typing its name followed by ".com." Second-level domain names became a tradable commodity. Name brokerages were set up, and a new class of name speculators registered hundreds of domain names and waited for businesses seeking an online presence to come along and buy them. Ones that were perceived as especially desirable were traded for thousands of dollars; several have changed hands for millions (Table 2). In a few thousand instances, name speculators registered popular trademarked brand names in the hope of attracting traffic to their businesses, or in an attempt to resell the name to the trademark owner. In a few cases, Internet sites used domain names to help confuse and exploit customers engaged in Internet commerce. (See MUELLER [1999] for a count and typology of domain name trademark conflicts.)

| Domain Name    | Price (US\$)   | Year |
|----------------|--|------|
|                | * Price includes stock and/or future revenue sharing |      |
| Business.com   | \$7.50 million                                       | 1999 |
| Altavista.com  | \$3.35 million                                       | 1998 |
| Bingo.com      | \$1.10 million*                                      | 1999 |
| Wallstreet.com | \$1.03 million                                       | 1999 |
| Rock.com       | \$1.00 million*                                      | 1999 |
| Eflowers.com   | \$1.00 million*                                      | 1999 |
| University.com | \$530,000  | 1999 |
| Computer.com   | \$500,000  | 1999 |
| Blackjack.com  | \$460,000  | 1999 |
| Business.com   | \$150,000  | 1997 |

**Table 2: Resale value of domain name registrations<sup>5</sup>**

If the commercial value of domain names was becoming evident, the economic value of domain names was dependent upon the Internet's root server system. Domain names derived their value as a globally visible locator from the existence of a coordinated, authoritative root

5 Source: Internet World, August 1, 1999, p. 29.

that kept track of where all names could be resolved and ensured that every name in use was unique. The value of the root, in turn, was almost entirely a product of network externalities.

The authoritative “A” root server operated by NSI under contract from the US National Science Foundation was accepted by computer networks all over the world as the uniform, authoritative source of information about where to resolve domain names. Anyone with computers and telecommunication links can set up an alternative domain name system. Unless the list of recognized top-level domains contained there is used by a critical mass of the world’s network administrators, however, the domain names registered in an alternate root will be invisible to most Internet users; that is, the names will not resolve. The existence of alternate, independent root servers thus raises a risk of fragmenting Internet connectivity. If registration information in an alternate root is not perfectly coordinated with the information in all other root server systems, domain names may not all be unique, or may not resolve properly. Thus, users and network administrators tend to converge on a *single* root. Alternate roots face the critical mass problem typically associated with services that have network externalities: competing roots have little value to users unless many other networks point at them. But no one has much of an incentive to point at them when they have so few users.

## **2. *Creating an Arena of Appropriation***

By 1995 it was evident that tremendous value inhered in the functions performed by a single, authoritative root of the Internet. Now various parties began to devise ways to capture some of that value, or to establish control over its source. An “arena of appropriation” was defined earlier as a site wherein business and political actors attempt to establish, via collective action, property rights in a new resource so that they can more securely exploit its value. Domain names and the root of the DNS became the focal point of appropriation activity from 1995 to 1998. The activity fell into two tracks: domain name-trademark interactions and demands to add new TLDs to the root.

### *a) Trademark-domain name conflicts*

Domain names can be business identifiers when used in a commercial context. From 1995 to 1997, World Wide Web URLs that included domain names began to appear frequently on television and in print. Many commercial domain names were taking on the characteristics of brand names. Online businesses such as *Amazon.com*, for example, came to be known by their domain names. Major corporations that had dismissed the Internet as an academic toy began to realize that the simple act of typing a name followed by *.com* could instantly deliver consumers to their web site. The growing perception that domain names possessed significant business value stimulated efforts to secure stronger property rights over them. Trademark law became the vehicle for these assertions.

But trademark law and domain names could not be mapped onto each other in any simple way. Domain names provided global visibility to a connected computer, and thus transcended jurisdictional variations in trademark law. Domain names are globally exclusive, but trademark law allows the same name to be used by businesses in different industry sectors. Litigation over

domain names often found businesses using trademark law in an attempt to wrest control of generic terms from legitimate registrants (e.g., *juno.com*, *clue.com*, *compassion.com*, *pike.com*). (OPPEDAHL [1999]) In trademark law, the key issues revolve around the subjective impact of the name; i.e., whether it confuses consumers or dilutes the value of a brand. Domain names, in contrast, are components of a technical system that requires of them nothing more than that they be unique character strings. Thus, to the DNS the names *amazon.com* and *amazom.com* are completely distinct and unique character strings and therefore pose no problems. To an end user and to trademark law, on the other hand, the names are highly similar and potentially problematic, especially if the latter is used to sell books online.

The different functions of the two approaches to naming resulted in radically different economics. Registering a trademark in one major jurisdiction such as the United States typically takes months and costs thousands of dollars. Patent and trademark offices carefully review the name before protection is granted. Gaining exclusive rights over a name that is international in scope takes even longer and requires more money. Registering a domain name with NSI, on the other hand, took a few hours and cost only US\$35 a year. There was no review process at all and the name was globally visible. The DNS, in short, created a global market for identifiers that was fast, cheap, and out of the control of traditional institutions.

To major corporate trademark holders, domain names were extensions of their brands and deserved protection as trademarks. To NSI and other prospective commercial domain name registration entities, domain names were just a commodity that could and should be sold in large quantities with no restrictions. And to many Internet users, an unrestricted, low-priced market for domain names facilitated free expression and inexpensive Internet visibility. Not all web sites were commercial; some choices of domain names (e.g., *scientology-kills.net*) raised freedom of expression issues. Any attempt to make domain name registration more like trademark registration would result in dramatically increased costs for end users and possibly a significant reconfiguration of the balance between free expression and trademark protection.

The ambiguity of the relationship between trademarks and domain names fostered extensive litigation among trademark owners, domain name registrants, and domain name registration businesses. (BURK [1995]; NATHENSON [1997]; RONY and RONY [1998]; OPPEDAHL [1999]; MUELLER [1999]). Trademark owners came into frequent legal conflict with innocent users who happened to have registered character strings that matched a trademarked name in some jurisdiction or industry. Trademark holders also went after “cybersquatters,” domain name speculators who sought to appropriate the good will in a recognized brand name by registering it as a domain name and reselling it (PANAVISION *v.* TOEPPEN [1998]). They also sometimes attempted to hold domain name registries responsible for contributory infringement (LOCKHEED MARTIN *v.* NETWORK SOLUTIONS [1997]). In such cases, they sought to shift the transaction costs required to protect their marks in the domain name space from themselves to the registration businesses, by requiring that the registries exclude names from databases or make judgements about the eligibility of a customer for a particular name.

b) *New TLDs*

The other problem that animated appropriation activity was the question of adding new top-level domains (TLDs) to the root of the Internet. As NSI happily collected a revenue stream approaching one hundred million dollars annually from registrations in the .com, .net and .org, TLDs, other companies began to ask why only NSI should be able to profit from the business. As noted before, the existence of only three generic TLDs open to unrestricted registration was an entirely arbitrary limitation. From a purely technical standpoint adding new names to the root is not complicated at all; it involves little more than adding text to a list. Nevertheless, the prospect of such additions raises complex questions about property rights and public policy:

- Who has the authority to add names to the root?
- How many new TLDs should be or could be added? If limits must be imposed, how does one decide who gets to administer a new TLD and who doesn't?
- If there are competing applications, for the same TLD, how does one decide which applicant gets it?
- Should the root server administrator profit from the addition of new TLDs; e.g., by charging a fee, auctioning off the right, or demanding a percentage of revenues?
- Can there be intellectual property in a TLD string? Do those rights inhere in the registrant or the registry?
- What are the property rights of the administrator of a TLD domain? Do they "own" the right to enter registrations under the TLD, or must they share the right to perform registrations with other companies? Do they own the zone files? Who owns the registration database?
- Will the addition of new TLDs create additional headaches for trademark owners who have already registered their names in existing domains? If a successful business was established at [www.shop.com](http://www.shop.com), what happens when [www.shop.web](http://www.shop.web) or [www.shop.inc](http://www.shop.inc) become available?

These problems also led to litigation and other kinds of appropriation activity. NSI attempted to establish permanent control over the authority to register names under the .com, .net and .org domains, while the Internet Society tried to assert administrative control of the root in order to gain authority over when and how TLDs could be added. (These efforts are discussed in detail below in the section on bootstrapping.) Some entrepreneurs tried to create new, competing root server systems that recognized new TLD names (RONY AND RONY [1998], 543-6). There was also an antitrust lawsuit against NSI and NSF over restrictions on the addition on new TLDs to the root (PGMEDIA [1999]). The Internet was also becoming a global medium, and the value and importance of the root led to expressions of concern from other national governments and international organizations that the issues be considered in an international context and not as a purely domestic matter by the United States.

Both problems described above (new TLDs and trademark-domain name conflicts) were not resolved within the established institutional regime. Instead, the conflicts culminated in the formation of a new institutional framework, spearheaded by a new international organization, the Internet Corporation for Assigned Names and Numbers (ICANN). Institutional innovation was the product of necessity, not choice, and of conflict and controversy rather than consensus and harmony. The next two sections describe the bootstrapping problems and the existence of a major conflict over the distribution of transaction costs, both of which acted to prevent resolution of the issues within existing frameworks.

### **3. *The bootstrapping problem***

A bootstrapping problem exists when there are substantial uncertainties about who among existing organizations has legitimate authority to establish, recognize, or enforce property rights. The Internet domain name space suffered from this problem severely. Who really owned the DNS root? Or, for that matter, the IP address space? The short answer is that before 1994, no one worried about that question. Formal legal control of the name space had not been relevant during most of the Internet's history. For nearly twenty years, the Internet had developed as a subsidized research and education network. Most of the coordination of the name and address space had taken place amongst non-commercial actors whose income came from grants. As subsidized technologists, their rewards came from operational results; hence, they had every incentive to cooperate in the construction and interconnection of networks and little reason to worry about appropriating the commercial value of the Internet name space. Prior to 1994, moreover, there was no apparent commercial value to be appropriated.

The rapid emergence of the Internet as a global medium, the institution of charging for domain names in 1995, and the subsequent clamor to add new TLDs to the root suddenly altered this situation. The act of adding TLDs, as noted above, raised difficult economic, policy and legal questions. Those questions could not be answered unless someone exercised formal legal authority over the root of the domain name space. Yet, as the following historical narrative shows, once formal legal authority over the root was at stake, the informal cooperation among many internationally distributed parties that had worked so well at developing the Internet collapsed into warring factions.

The key actors in this process were the two major US government contractors who held de facto control of the name and address assets:

- The Internet Society, which hoped to gain permanent administrative control over the root of DNS and the IP address space, and
- NSI, which hoped to turn its government contract to run the globally popular com, net and org TLDs into a permanent private property right

Unfortunately, both organizations came to view the other as the main threat to the accomplishment of their agenda. A bitter split developed within the ranks of the Internet operational community. This reinforced the bootstrapping problem, as each would oppose any attempt by the other to assert authority or gain control. The next sections describe the series of

failed attempts to establish formal authority over the root that took place between 1994 and 1998.

a) *First attempt to control the root: moving IANA into ISOC*

The first attempt to establish formal, private control of the root came from the Internet Society (ISOC) in 1994. The Internet Society (ISOC) was a non-profit membership organization formed by Vinton Cerf in 1992 to consolidate control over Internet standards administration. (Cerf was one of the co-developers of the IP protocol.) Jon Postel, another Internet pioneer closely linked to Cerf and ISOC,<sup>6</sup> had managed the administration and editing of the “Request for Comment (RFC) series” documenting Internet standards since the early 1970s. Postel worked at the University of Southern California’s Information Sciences Institute (USC-ISI). With funding support from DARPA, Postel also handled most of the early domain name and address administration. His activities came to be known as the Internet Assigned Numbers Authority (IANA). In July 1994, Postel prepared a charter proposing to transfer ownership of the IANA function from a government contract with USC-ISI to the Internet Society, and circulated it among the Federal Networking Council. (RUTKOWSKI [1998]) In proposing to transfer the IANA function into a private organization, Postel sought to provide for his operation a more secure and independent legal and financial footing in the new commercialized environment. Postel’s proposal, however, prompted debate within the federal government agencies involved in the Internet about whether ISOC possessed the “jurisdiction and overall responsibility” for the domain name space. (RUTKOWSKI [1998]) The questions were never resolved, and no formal transfer of authority took place, although IANA began to refer to itself as an organization “chartered” by the Internet Society.

b) *Second attempt to control the root: Postel’s new TLD proposal*

Network Solutions, Inc. (NSI) was a commercial, for-profit corporation. Its five-year Cooperative Agreement by the National Science Foundation (NSF), which started in 1993, gave it control of the InterNIC, the headquarters of the central domain name registry and authoritative root server system. Unlike IANA, it did not have longstanding ties to the Internet technical community. Indeed, shortly after NSI was authorized to begin charging for domain name registrations it was acquired by a \$4 billion defense and technology conglomerate, Science Applications International Corporation (SAIC). The rapidly growing revenue stream generated by the charging decision allowed NSI to make an initial public stock offering in 1997. NSI’s commercial exploitation of domain name registrations did not make it popular with the traditional Internet technical community. In September of 1995 Postel expressed his view that there should be competition with NSI.<sup>7</sup>

---

6 Postel was a founding member of the Internet Architecture Board and served continuously from its founding until his death in October 1998. He was the first individual member of the Internet Society. V. Cerf, “I Remember IANA,” RFC 2468, October 1998.

7 Email, Postel to ISOC trustees, 15 Sep 1995; stored on Rutkowski [1998] WIA web site.

Postel drafted a proposal that would have added up to 150 new, “descriptive” TLDs over a period of three years. Each of the TLDs would be managed by competing, proprietary registries that paid a fixed fee of \$2,000 a year plus 2 percent of the income from registrations into a fund managed by the Internet Society.<sup>8</sup> ISOC’s board endorsed the plan in June 1996. Once again, IANA and ISOC were proposing what was in essence a privatization of the root without any formal legal authority. Moreover, it was evident that they viewed administration of the root as a money-spinner that would provide long-term financial support for their organizations.

IANA/ISOC’s second assertion of authority was not successful. The proposal encountered vocal opposition from a variety of interest groups. The strongest opposition came from trademark owners’ associations. The trademark lobbying groups strenuously objected to the expansion of the name space because they feared that it would increase the scope for trademark conflicts, name speculation and dilution. A staff member of the International Telecommunication Union (ITU), an organization that viewed itself as the natural home for administration of global network resources, publicly criticized the plan, charging that IANA lacked the authority to “tax the root.”<sup>9</sup> Postel even failed to win the support of the prospective domain name registration businesses that wanted to operate new TLDs. These businesses complained about the fees required to enter the market and IANA’s lack of legitimate authority to assess them.<sup>10</sup> By fall 1996 it was clear that IANA and ISOC possessed neither the legitimacy nor the legal authority needed to administer a global resource of such importance. In their next attempt, however, IANA and ISOC were much more ambitious.

*c) Third attempt to control the root: The IAHC and the gTLD-MoU*

In October 1996 the Internet Society seems to have recognized that if they were to succeed in their mission to gain control of the root they would have to break new institutional ground. ISOC put together what it called a “blue ribbon international panel” to develop a plan.<sup>11</sup> Its initiative reflected its continuing desire to assert its authority to administer the root, but extra urgency was added by the threat that the growth of alternative roots might fragment Internet connectivity.

The 11-member committee chaired by ISOC CEO Don Heath, dubbed the “International Ad Hoc Committee” (IAHC), represented a coalition among ISOC and its most powerful critics from the previous round. Trademark owners and ITU were incorporated into the planning process, and later would be given permanent roles in a new governance system. IAHC contained two representatives of large trademark holders appointed by the International

---

8 Originally, Postel had proposed a \$100,000 fee plus 2% of revenues, but the squeals of outrage prompted a quick reduction in successive drafts.

9 G. Lawton, “New top-level domains promise descriptive names,” SunWorld Online (September 1996).

10 Ibid.

11 News Release, ISOC, WASHINGTON, DC, October 22, 1996 “Blue Ribbon International Panel to Examine Enhancements to Internet Domain Name System.”

Trademark Association (INTA) and the World Intellectual Property Organization (WIPO). The ITU staff member who had criticized the earlier Postel draft was invited to be on the Committee. So was a representative of the NSF. The committee also contained five IETF/ISOC technical members selected by Postel.

The IAHC charter was released Nov 11, 1996, and public comments were solicited via email. Only three months later, a Final Report laid out a new system of Internet governance (IAHC [1997]). The IAHC Final Report embodied a new conception of the domain name space as a “public resource.” (RUTKOWSKI [1998]; SIMON [1998]). It also proposed a structural model for the domain name registration business that diverged significantly from current practices of NSI. The IAHC plan conceived of the registry database as a natural monopoly, and sought to separate the “wholesale” operation of the monopoly registry database from the “retail” function of registering names for customers, billing them, and maintaining contact information. The former function was called the “registry” and the latter the “registrar.” Under the IAHC plan a single, monopoly registry would be administered on a non-profit basis. The registry would be co-owned by multiple, competing registrars, who would all share access to the same TLDs.

Another dramatic difference was that the new system proposed by IAHC linked trademark protection procedures directly to the administration of the DNS. This important but controversial innovation was clearly meant to eliminate the trademark owners’ objections to new TLDs by giving them extraordinary power over domain name registrations. Domain names would not be operational until after a 60-day waiting period, during which they would be subject to review by “Administrative Challenge Panels” run by WIPO. Neither the law nor the legal principles WIPO would use to resolve disputes were specified. IAHC also proposed to exclude from the domain name space all names that corresponded to or resembled “famous” trademarks. Where Postel had originally thought in terms of hundreds of new descriptive TLDs, IAHC proposed to add only seven.<sup>12</sup> This, too, was a concession to the trademark interests. The smaller the name space, the easier their policing problem. Thus, the IAHC expanded the name space slightly but treated it as a regulated cartel.

The IAHC also established a complicated governance structure that straddled the boundary between the public and private sectors. The overarching framework of the governance structure was a document known as the Generic Top Level Domain Memorandum of Understanding (gTLD-MoU). Registrars would be incorporated in Geneva as a non-profit Council of Registrars (CORE). To join CORE, registrars had to pay a \$20,000 entry fee and \$2,000 per month, plus an anticipated but as yet unspecified fee for each domain name registration. The top governance authority was a committee designated as the Policy Oversight Committee (POC). POC’s membership mirrored the composition of the IAHC: two members were to be appointed to it by ISOC, the Internet Architecture Board, IANA, and CORE; one member was to be appointed by ITU, INTA, and WIPO. In formulating policy the POC would issue requests for comments just as a regulatory commission might. There was also a Policy Advisory Board (PAB), a consultative body that any signatory to the gTLD-MoU could join.

---

12 The seven proposed gTLDs were: .web, .info, .nom, .firm, .rec, .arts, .store.

The gTLD-MoU was signed by Heath and Postel March 1, 1997. ISOC and ITU then organized an official signing ceremony in Geneva in an attempt to assume all of the trappings of an international treaty agreement. Members of the IAHC conducted an international series of promotional meetings and press releases to win acceptance of the proposal. Yet ISOC and IANA still had no more formal legal authority over the root than they had had in mid-1996.

ISOC and IANA's assertion of authority failed again, but this time the bold creation of a new institutional framework was enough to send ripples through the international system. The highest levels of the US Government began to pay attention. NSI, which correctly saw its control of the lucrative .com domain as the target of the gTLD-MoU's shared registry model, mounted a lobbying campaign against the proposal. The Internet entrepreneurs positioning themselves as alternative registries opposed the plan because it limited TLD expansion to a monopoly registry, and imposed heavy fees and regulations upon participating registrars. Many policy analysts and user groups criticized the gTLD-MoU as a sellout to the trademark interests. Many trademark holders, however, were unhappy with the creation of any new TLDs and criticized INTA for its participation. The European Commission weighed in against the plan, charging that it was "too US-centric" and demanded more EC representation and "further public debate." The US government executive branch was not pleased with the involvement of the ITU.<sup>13</sup> Congressional hearings were held, during which Republican critics focused on the gTLD-MoU's plan to move authority out of the United States.<sup>14</sup> The seven proposed new gTLDs were never added to the root, and the 80-odd companies that had paid fees to become CORE registrars saw nearly a million dollars evaporate.

d) *Other indications of a bootstrapping problem*

The most dramatic examples of the bootstrapping problem were attempts to directly seize the Internet's central administrative functions. There were two such attempts, one in July 1997 and another in January, 1998. In the summer of 1997 Eugene Kashpureff, operator of a competing root server system known as AlterNIC, successfully implemented a network "hack" that redirected all Internet traffic bound for NSI's registry to his own AlterNIC site. (Diamond [1998]) Kaspureff's hijacking was more an act of political protest against the NSI monopoly and the failure to recognize new TLDs than an attempt to permanently appropriate control of InterNIC domain name registrations. But it did demonstrate the vulnerability of the Internet's central functions and the existence of challenges to its legitimacy.

A more significant demonstration of the lack of authority over the root server system occurred on January 29, 1998. Apparently concerned about the direction US policy was taking, Jon Postel conducted what he referred to as a "transition in management arrangements" and

---

13 In late April 1997 US Secretary of State Madeline Albright wrote a memo criticizing the ITU Secretariat for acting "without authorization of member governments" to hold a "a global meeting involving an unauthorized expenditure of resources and concluding with a quote international agreement unquote."

14 U.S. House of Representatives, Committee On Science, Subcommittee On Basic Research, Hearing on Internet Domain Names, 30 September, 1997.

later called a “test.” Others referred to it as a hijacking of the root. Postel initiated a change in the algorithm by which the 12 geographically distributed root servers loaded their contents. Based on instructions from Postel, eight of the 12 root servers were modified to take their authoritative zone files from Postel instead of the “A” root server operated by NSI.<sup>15</sup> Clearly, the claim to “authoritative” root server status was in play. The implications of a coordinated redirection of the root were not lost on anyone. Although he did not do so, Postel *could have* added to the root server system the new gTLDs proposed by the gTLD-MoU. Had he done so, however, the result would have been two different Internet roots, possibly fragmenting Internet connectivity.<sup>16</sup>

Conspicuous by their absence in the narrative above are the higher-level policy-making and legislative branches of the US government. The US government had created the Internet protocol and was the contracting authority behind both IANA and NSI. Why hadn't it acted to resolve the property rights questions? There are two answers.

- Although the fast pace of Internet development required quick action, the DNS problem in the 1995-6 time frame was too obscure to attract the attention of the US Congress or the executive branch. Equally important, the issues raised were far too new and technical for most ordinary policy makers to understand. That left the initiative in the hands of lower-level players. These lower-level actors could make decisions that affected Internet administration in important ways, but they did not have the authority to make public policy or law.
- Even if the higher levels of US government had been fully aware of the problem, their authority over the Internet had been eroded by its international diffusion and commercialization. Operationally, the delegation of de facto property rights over names and addresses to organizations outside the US limited the US governments' freedom of action. More importantly, their legitimacy as the ultimate decision maker was diminished by the creation of many international stakeholders in the Internet. Indeed, when the US government did officially intervene (see below) its authority to do so was strongly challenged by the gTLD-MoU parties, who claimed that “some in the international Internet community view the Green Paper as an unlawful attempt by the U.S. Government to claim ownership of the Internet.”<sup>17</sup>

---

15 Root servers B, C, D, F, I, K, L, and M – the servers at universities and research institutes, including RIPE and Nordunet in Europe – participated in Postel's “test.” Servers E, G, H, and J – the ones at NASA, the US military network, the Ballistics Research Lab, and NSI – did not.

16 For news coverage of this event see Sandra Gittlen, “Taking the Wrong Root?” *Network World*, Feb. 4, 1998; Ted Bridis, “Clinton administration says Internet reconfiguration was rogue test,” *Associated Press*, February 5, 1998.

17 Official Comments on the Green Paper (Technical Management of Internet Names and Addresses) from the Internet Council of Registrars (CORE), March 23, 1998, <http://www.corenic.org/documents/official.htm>

Internetworking by means of TCP/IP is characterized by a widespread distribution of responsibility. Although NSI was responsible for administering the authoritative “A” root server, there were 12 other root servers distributed around the world, some operated by IANA, some run by military agencies, and some administered on a voluntary basis by universities both inside and outside the United States. Although all of them took the authoritative root zone file from the “A” server, that was an act of voluntary compliance, as Postel’s “test” had revealed.

IANA had fairly direct control over allocation and assignment of the IP address space, but beginning in 1990 it had delegated large blocks of IP addresses to a regional registry in Europe, and later to an Asia-Pacific registry. Both were authorized to sub-delegate IP address blocks to Internet Service Providers and large users within their region.<sup>18</sup> Significant chunks of the address space were, therefore, no longer directly under the control of the US government or even IANA.<sup>19</sup> The same distribution of authority had occurred in the top level of the domain name space. From 1985 to 1997 IANA delegated the authority to administer two-letter country codes (ccTLDs) to nationals within the referenced country (POSTEL [1994]). Those delegations gave organizations outside the United States responsibility for administering over 200 TLDs. Such *de facto* property rights could not have been recalled or altered without major geopolitical conflict and possibly even operational disruption of the Internet.

#### **4. Distributional conflicts**

As noted above, when new forms of property are created there can be political and legal conflict over the distribution of costs and benefits. By winning acceptance of novel institutional arrangements, a coalition of organizations may put into place a distribution that is highly favorable to themselves and can last for a long period of time. Conflict over the distribution of transaction costs was endemic to the interaction between domain names and trademarks. The issue was perceived to be of very high stakes by the trademark holders.

Trademark owners complained that the DNS massively increased the cost of policing and protecting their marks. Multinational companies with famous brand names discovered 20-30, and sometimes over 100, domain names that incorporated character strings they considered infringements of their marks. DNS seemed to lower the threshold of infringement to absurd levels. The name speculator who registered “*exxonmobil.com*” just after news of the merger between the two oil companies, for example, spent only \$70 and a few minutes. To track him down and engage in a lawsuit, on the other hand, would run in the tens of thousands of dollars. In some cases, a name speculator may be difficult to track down even if a company was willing to assume the costs of litigation. Many registries did not verify the accuracy of the contact

---

18 In Europe, the regional address registry was Reseaux IP European (RIPE). Later, similar authority was delegated to an Asia-Pacific registry, APNIC. In 1998, a third address registry was created for the Americas, ARIN.

19 In some early (1995) debates about name and address space ownership, for example, a RIPE member warned a US official, “it would be very interesting to see the US Government assert ‘rights’ to the address space allocated to non-US regional registries or assigned to non-US end users.” Rutkowski 1998.

information in the domain name registration record. Indeed, when domain name registrations were exploding in 1995 and 1996, NSI often failed even to bill the domain name registrant for many months, which meant that hundreds of names could be registered for free.

There was some truth to the cries by the trademark lobby, but they overlooked a far more important fact about the DNS and its relationship to intellectual property in names. Although DNS did dramatically lower the cost of acquiring names, it also drove down to unprecedented lows the cost of monitoring names and tracking when, where, how, and by whom they were used. Trademark owners could perform automatic searches in the DNS database to detect whenever domain name registrations matched marks.<sup>20</sup> They could find their name in any combination or form they wished. More comprehensive intermediary services capable of searching registrations across all country code TLDs quickly emerged in the marketplace.<sup>21</sup> Name registrations could be monitored and challenged almost as soon as they were put into use. The usage of the domain name as a web site was immediately visible to anyone in the world with Internet access.

Prior to the Internet's creation of an arena of global electronic commerce, it would have taken months of labor-intensive searching to discover and take action against so many uses of a name over such a wide geographic area. Many violations simply never would have been discovered at all. There is, after all, no globally centralized database where every business in the world must register their names. Pirate operations that produce and sell physical merchandise with phony brand names do not have to register with anyone at all. Thus, Internet "pirates" are far more traceable than their physical world predecessors. In fact, it was the superior monitoring capabilities of the Internet that made the domain name issue attract so much attention among the intellectual property community.

A capacity to centralize distributed information is the computer's great contribution to the reduction of costs associated with protection of intellectual property. The databases of Internet names and numbers not only allowed trademark owners to instantly identify such registrations, it also gave them information about the date of registration, name, technical contact, and email address of the person whose registration they wished to challenge. Any registrant could in principle be visible, no matter how miniscule the size of their business, or even whether they had a web site up and running at all. True, the current procedures for domain name registration were imperfect from the trademark holders' point of view. The contact information could be false or out of date, and there was no uniform, inexpensive dispute resolution venue where registrants could be challenged. But it was clear that the Internet's centralization of

---

20 The "WHOIS" service of the Internet allows the database of registered names to be searched by person registering or by names. The InterNIC web site allows WHOIS searches to be done on domain names or users, See <http://www.networksolutions.com/cgi-bin/whois/whois>

21 The "Saegis" service offered by Thomson and Thomson, an intellectual property management firm, can provide brand name holders regular reports on domain name registrations in every TLD in the world for any specified character string that include the domain name.

identification information offered huge opportunities for lowering their transaction costs and expanding the scope of their property rights, if it could be exploited suitably.

In line with this realization, the trademark interests began to advocate legal and policy positions that would engineer a major shift of transaction costs in cyberspace. Several lawsuits tried to make domain name registration authorities responsible for screening names by accusing them of “contributory dilution,” thus shifting the burden of policing away from the trademark holder and on to the registry (*Lockheed v NSI* [1997]; *Domainz* [1998], *Worldsport V. Art Internet S.A.* [1999]). The trademark interests, however, viewed litigation as expensive and burdensome. They wanted protection to be “built in” to the domain name registration process so problems would be prevented rather than remedied after the fact.

Legal pressure from trademark holders prompted NSI in 1995 to institute a “dispute resolution policy” to protect trademarks. The policy allowed NSI to suspend one of their customer’s domain names after a 30-day notice if a trademark owner showed that their mark exactly matched the second-level domain name, and if the registrant could not also show that they had a trademark on the name. The mechanical matching of names, however, resulted in the expropriation of domain name registrants engaged in noncommercial use, and small businesses that were engaged in legitimate concurrent use of a name. The NSI policy did not satisfy the trademark owners, either. From their standpoint it was underinclusive because it did not allow them to challenge names that were similar but not identical to marks.

Trademark lobbyists actively lobbied against the creation of any new TLDs as well (Moskin [1998]; INTA [1998]). Blocking the creation of new TLDs reduced trademark owners’ transaction costs by artificially restricting the name space, thereby reducing the opportunities for new problems. But in doing so, it imposed opportunity costs on the many businesses that were willing and able to enter the registry business, and upon innocent consumers who wanted to register new, and perfectly legal domain names. By most estimates, less than one half of one percent of all domain name registrations are problematical from a trademark perspective. (Mueller [1999]; WIPO [1999], Annex IX)

In the courts, trademark holders met with limited success in their broader agenda. Court rulings were uniformly hostile to pure domain name speculators, and intellectual property holders succeeded in recovering their names. (Mueller [1999]) Legal attempts to require the domain name registries to screen, exclude or otherwise police trademarked names were unsuccessful, however. Landmark cases in the US such as *Lockheed* and the *Oggi* case in New Zealand (*Domainz* [1998]) resulted in decisions absolving registries from liability for the actions of domain name speculators or infringers.

The trademark lobby thus began to turn to *institutional* methods of reducing their transaction costs. The pioneer of this approach was the gTLD-MoU proposal, which attempted to structure DNS administration in a way that tied it directly to trademark exclusions and domain name challenge and dispute resolution procedures. In December 1998 a World Intellectual Property Organization proceeding produced an *Interim Report* on Internet domain names. (WIPO [1998]) The report revealed that WIPO and its constituency, the major multinational intellectual property holders, were fully aware of the tremendous opportunity for

shifting transaction costs that could come with domain name policy. The DNS database not only offered a point of centralized surveillance of Internet users, it also offered administrators the leverage for enforcement: the withdrawal of a domain name. (As Post [1998] has observed, withdrawing a domain name constitutes a kind of banishment from cyberspace.) The WIPO report strained for the strongest intellectual property regime imaginable. The essential features of the report were:

- Secure complete and accurate contact information from all domain name registrants, and make the use of false, misleading, or inaccurate registration information grounds for forfeiting a domain name, even without any intellectual property violation.
- Make the databases containing all contact information of domain name registrants publicly available regardless of privacy considerations, so that IPR holders can use it to issue effective legal challenges to any domain name registration in the world.
- Create a new system of global administrative law to protect IPR on the Internet. WIPO proposed instituting an arbitration process to adjudicate domain name disputes; all domain name registrants would be contractually bound to submit to the process when they registered a name. Rather than applying existing national or international laws, WIPO proposed to develop its own rules for settling disputes between IPR holders and domain name users. The one-sided procedure virtually encouraged domain name hijacking by experienced, well-funded multinational trademark lawyers, whose challenges would pose formidable risks and uncertainties to an average domain name registrant. (Froomkin [1999]) Challengers who lost in the arbitration could revert to a court; losers in most cases could not. By positioning itself as the dispute resolution service provider, WIPO stood to benefit economically from the proposal.
- Extend WIPO's proposed adjudication procedures to every type of intellectual property dispute involving the Internet, including rights of personality and copyright as well as trademark; WIPO ceased using the word "trademark" to describe the object of the proceeding and used "intellectual property" instead.
- Define procedures to allow WIPO to recognize and protect "famous" trademarks by excluding them from the DNS database in all TLDs. Famous mark holders would only have to pay a one-time fee reflecting administrative costs to obtain these exclusion rights in perpetuity.

The WIPO interim report's recommendations were opposed by existing and prospective registries, organizations representing the Internet technical community and many individual domain name holders.<sup>22</sup> Although the widespread opposition forced WIPO to modify its

---

22 Critical comments were received from ISOC, the Association for Computing Machinery, the US Small Business Administration, a letter from 60 signatories represent a diverse group of law professors, academics, students, attorneys and industry leaders, and many individuals. Public comments on WIPO's Interim Report (RFC 3) can be viewed at <http://ecommerce.wipo.int/domains/process/eng/processhome.html>. Visited

proposals significantly,<sup>23</sup> the Interim Report is valuable as an indication of the specific distribution of transaction costs hoped for by the intellectual property interests.

### **5. Institutional Innovation**

Thus, both of the key property rights problems—bootstrapping and a major conflict over the distribution of transaction costs—were present as an arena of appropriation was formed around the Internet root in the mid-1990s. I now examine how engagement with these problems led to institutional change.

The real seed of institutional innovation was the IAHC's 1997 attempt to create a new governance structure independently of the US government. An initiative of the Internet Society and IANA, the gTLD-MoU established both the basic policy/legal model for the new institution and obtained a first-mover advantage in building the international alliances needed to support it. It brought trademark interests directly into the domain name governance process and offered them controls over domain name registrations and limits on the name space. It engaged two international organizations (ITU and WIPO), both of them palpably eager for a seat at the Internet governance table. Furthermore, it offered new business opportunities to non-US companies. Its plan to create seven new TLDs and to distribute the right to register domain names in them among registrars in different regions of the world seemed attractive to foreign companies who were otherwise shut out of the domain name registration business. Obviously, the coalition intentionally excluded and isolated NSI, as well as the North American prospective registries who had hoped to operate new, proprietary registries.

The fatal weakness of the gTLD-MoU was its soft support from the US government. Nominally, the National Science Foundation (NSF) was a part of the IAHC and participated in the definition of its Final Report. However, NSF lacked the authority to enter into international agreements and lacked the direct backing and policy guidance of the White House in this case. The prominent role of the ITU in the gTLD-MoU was bound to antagonize elements of the US government, which did not want the Internet to become incorporated into the more formal, state-dominated telecommunications regime. Ironically, the gTLD-MoU also lacked support from European and Asian governments for precisely the opposite reason: many saw it as a US-based initiative and did not approve of its private-sector-dominated approach. Thus, as the decision-making authority elevated to the level of governments and international organizations, significant issues regarding the transfer of authority needed to be worked out.

---

October 1999.

23 In its Final Report, issued April 30, 1999, WIPO retracted the focus of its compulsory ADR process, restricting it to "abusive registrations," and confined its focus to trademark concerns rather than intellectual property in general. The arbitrators were also instructed to apply national laws whenever possible. The revised proposals still gave IPR holders access to complete and accurate information about domain name registrants, a uniform and mandatory dispute resolution procedure, and retained procedures to protect famous trademarks.

In July 1997 the US government, prompted partly by the GTLD-MoU controversy, partly by the complaints of trademark owners, and partly by the impending expiration of the NSI and IANA contracts, initiated an official proceeding on administration of DNS.<sup>24</sup> A Presidential Executive Order authorized the Secretary of Commerce to “support efforts to make the governance of the domain name system private and competitive and to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis.”<sup>25</sup> In issuing the Notice, the USG asserted its ultimate authority over IANA and the DNS root, but also indicated its intention to relinquish that authority in a way that involved Internet stakeholders internationally. The lead authority for DNS policy was moved out of the National Science Foundation and into the Department of Commerce.

After two rounds of public comments, the Clinton administration released its final plan, the so-called White Paper, on June 3, 1998. (DEPARTMENT OF COMMERCE, NTIA [1998]) Nominally, the White Paper proposed a method of privatizing the name and address space that relied on “private sector leadership.” The document set out some guiding principles and policy objectives, but insisted that the private sector itself must form a new non-profit corporation to administer the Internet’s name and address space. The US Commerce Department would then recognize this corporation and, over a two-year period, transfer to it the functions of IP address space allocation, protocol parameter assignment, domain name system management, and root server system management.

Underneath the rhetoric of “private sector leadership,” however, the US government tried to resolve the political problems by making agreements with some of the key players about how the process would work. The US decided that the core of the new organization would be formed around IANA/ISOC and its allies, which now visibly included IBM and principals in the major US law firm Jones, Day, Reavis and Pogue. Jon Postel and Joe Sims, his Jones Day lawyer, drafted articles of incorporation and by-laws for an “Internet Corporation for Assigned Names and Numbers” (ICANN). After the release of the White Paper Postel and Sims, in consultation with ISOC, Magaziner, IBM, and European and Asian governments, quietly selected the nine initial Board members. In November 1998 the Commerce Department officially recognized ICANN and its Board as the organization that would inherit the responsibility for managing names and numbers.<sup>26</sup> The new Chief Executive Officer of ICANN, Mike Roberts, was an ISOC veteran and gTLD-MoU partisan.

---

24 Request for Comments in the matter of Registration and Administration of Internet Domain Names, U.S. Dept of Commerce Doc. No. 970613137-7137-01, 1 Jul 1997.

25 A Framework for Global Electronic Commerce. The White House. July 1, 1997. <http://www.ecommerce.gov/framework.htm> Visited October 7, 1999. Presidential Directive on Electronic Commerce, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, 1 July, 1997, <http://www.ecommerce.gov/presiden.htm>.

26 <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>. Visited October 1999.

In giving official sanction to ISOC/IANA, however, the USG also made important concessions to other governments. At the insistence of the Europeans, the White Paper gave WIPO a formal role in the process. It called upon WIPO to initiate a “balanced and transparent process” to develop recommendations in three areas:

- A uniform approach for resolving trademark-domain name disputes involving “cyberpiracy”
- A process for protecting famous trademarks in gTLDs
- An evaluation of the effects of adding new TLDs on trademark and intellectual property holders.

European and some Asian governments insisted that even if Internet administration was to be privatized, there had to be some formal channel for governments to be involved.<sup>27</sup> This led to the creation of ICANN’s Government Advisory Committee (GAC), which offered governments and the national PTT regulators who participated in the ITU a special role within ICANN.

ICANN’s formal structure is diagrammed in Figure 1. ICANN is a California non-profit organization governed by 18 volunteer Directors and a salaried CEO who sits on the Board of Directors ex-officio. Members of ICANN’s Board of Directors are selected in four distinct ways. Three Supporting Organizations (SOs), each one representing a separate functional area of Internet management, elect three Directors. Eventually, the nine at-large board members will be elected by ICANN’s at-large membership. As noted in the previous section, ICANN also has a Government Advisory Committee (GAC) which serves as a formal channel for communication and influence between national governments and ICANN’s staff and Board.

The ICANN Bylaws called for three Supporting Organizations, one concerned with domain names (the Domain Name Supporting Organization or DNSO), one concerned with IP address management (the Address Supporting Organization or ASO) and the third concerned with protocol parameter assignment (the Protocol Supporting Organization or PSO). The ASO is nothing more than an extension of the regional address registries and the PSO is basically controlled by the IETF.

The DNSO was recognized from the outset as the most difficult to form, because of the ongoing power struggles over domain name policies. Had ICANN followed the pattern set by the other SO’s, it simply would have made the DNSO an organization of domain name registries such as NSI and the ccTLD operators. Because registries in general and NSI in

---

27 “[T]he European Commission is seeking a clear role for the international organisations such as WIPO and ITU in international communications policy. The Internet is not an exception. We regard the statement in the White Paper as a minimum role, which should be implemented in the Bylaws of the new organisation. I notice that the current draft Bylaws include a provision for Advisory Councils, and there may be a solution to be found in that context.” C. Wilkinson, European Commission “Internet Governance - Implementation of the US White Paper.” Internet DNS Summit, Geneva, 24 July 1998. <http://www.ispo.cec.be/eif/dns/cwgeneva.html>

particular were objects of such controversy, however, the ICANN Board instead made the DNSO into a quasi-representational policy making forum. DNSO is composed of a Names Council, a General Assembly, and various Constituency Groups representing DNS-related interests. The seven constituencies are shown in Figure 1. Each constituency elects three members of the DNSO Names Council which is supposed to manage the DNSO's consensus building process and communicate recommendations about Domain Name System policy to the ICANN Board of Directors.

ICANN's status as an institutional innovation should be evident. Nominally a private corporation, it has been delegated authority over global resources that are critical ingredients in gaining access to the Internet: domain names and IP addresses. Its formation required an international agreement, albeit an unusually informal one, among national governments, international organizations, commercial private sector actors, and some representatives of civil society. Because its control of an exclusive resource raised widespread concerns about its accountability, ICANN created a membership structure and formal bureaucratic mechanisms for the representation of various interest groups, and adopted formal notice and comment procedures that apply to all of its decision making. It also has numerous rules designed to assure geographic diversity in the election of officers and Supporting Organization council representatives. In short, ICANN behaves more like a regulatory agency than a private corporation or a typical industry standards-setting forum.

With the support of the US Department of Commerce, which still retains "policy authority" over the DNS root, ICANN has obtained the leverage to centralize contractual authority over domain name registrations in the most popular generic TLDs. Any domain name registry must contract with ICANN before its TLD name is listed in the root. All domain name registrars must also be accredited by ICANN before they can register domain names in the generic TLDs. This contractual relationship gives it the ability to tax and regulate key aspects of the domain name business. Registries and registrars pay fees that account for 90 percent of ICANN's budget.<sup>28</sup> Through the registrar accreditation contracts, ICANN extends its regulatory control to domain name users, because each registrar passes on the conditions and constraints of the ICANN contract to the domain name registrant.<sup>29</sup>

The centralization of authority via contract has allowed ICANN to implement a compulsory "uniform dispute resolution policy" (UDRP) for resolving trademark-domain name

---

28 ICANN Task Force on Funding, Draft Final Report, October 30, 1999, posted at <http://www.icann.org/tff/final-report-draft-30oct99.htm>

29 ICANN's authority over the IP address space is weaker. The IPv4 address space has already been delegated to the existing RIRs. The much larger address space created by the new IPv6 protocol was also delegated to the RIRs in Summer 1999. According to the MoU with ICANN, the ASO's responsibilities "do not extend to the business practices or local policies of the RIRs except as needed to ensure that the RIRs meet the criteria for ICANN approved RIRs. The RIRs are responsible to their own members and in most cases this must be their prime responsibility." See Memorandum of Understanding, ICANN Address Supporting Organization, <http://www.aso.icann.org/docs/aso-mou.html>

conflicts, as proposed in the WIPO Final Report [1999].<sup>30</sup> Though the UDRP is based on the final WIPO recommendations, the interaction of the seven constituencies in ICANN's DNSO resulted in changes that made it slightly more favorable to individual domain name registrants. ICANN has thus created a global system of administrative law that can serve as an alternative to national law. An ICANN working group is also attempting to come up with a recipe for deciding how to protect globally famous names from cybersquatters. Once this work is concluded ICANN will have created new rights for multinational owners of brand names that might qualify for the appellation "famous." Another DNSO working group is developing proposals for if, when, and how to add new generic TLDs to the root. The significant point is that ICANN's DNSO is now the main arena for battles over the distributional issues related to trademarks and domain names.<sup>31</sup> Looking forward, ICANN will have helped to establish an infrastructure for the exploitation of domain name registration data for other regulatory purposes.

### III. Conclusions

The rise of the Internet fomented institutional innovation by creating a global resource that posed new property rights problems. Conflict over transaction costs, combined with a bootstrapping problem, created an opportunity for entrepreneurs within certain organizations to push forward a governance agenda. A coalition was formed between organizations seeking to assert administrative authority over the Internet (ISOC, ITU, WIPO) and organizations seeking to engineer into place long-term reductions in transaction costs (large, multinational trademark owners, intellectual property interests, and e-commerce interests). The process was relatively rapid. Although one could argue that the actual endowment of the Internet root took place gradually over a period of 15 years, once the property rights problems emerged around 1996 a new institutional framework for Internet governance took only three years to form. Of course, ICANN will continue to evolve and, given the controversial nature of its formation and the rapid pace of change in the Internet, its survival and success in its current form is by no means assured.

Both of the property rights problems identified in section 2—bootstrapping and conflicts over transaction cost distribution—were necessary elements of the recipe. The most important impetus for institutional change, however, was conflict over the distribution of transaction costs, and specifically, the desire of trademark holders to link the administration of domain name registration directly to the protection and enforcement of trademark rights.

---

30 The rules and procedures are posted at <http://www.icann.org/udrp/udrp.htm>. WIPO was the first organization to be recognized as a dispute resolution service provider under the UDRP; see <http://arbiter.wipo.int/domains/index.html>

31 The US Congress, however, still plays an important role. On October 26, 1999 it passed a new bill, H.R. 3028, that criminalized cybersquatting and created stronger forms of trademark protection in domain names.

The intellectual property interests refused to accept a system that allowed registries to assign domain names based upon purely technical or business criteria, and then use litigation in national courts to settle any subsequent trademark-related disputes over the names. Instead, they realized that their transaction costs would be greatly reduced, and the scope and efficiency of intellectual property protection in cyberspace greatly enhanced, if the root server database was fully leveraged as a tool for centralized surveillance and enforcement. The trademark interests insisted on directly linking the surveillance capability of the domain name database with policing and enforcement functions that, under traditional trademark practice, had to be performed at their own expense. That is, they demanded that the basic institutions under which domain name registration operated be re-engineered to facilitate monitoring and policing of their property.

That agenda could not be executed unless the Internet root was administered by an organization that transcended the limitations of national jurisdiction and was fully committed to the subordination of the domain name system to the protection of intellectual property. ICANN, the direct successor of the gTLD-MoU, fit the bill perfectly. Under ICANN's contracts with domain name registrars, the simple act of registering a domain name commits registrants to globally uniform dispute resolution procedures designed to protect trademarks. It provides intellectual property holders with complete and accurate contact information about any registrant, making legal challenges to a domain name easier than ever. The utility of the information is assured by a contract provision allowing the registry to take away the domain name if the information is not complete and accurate. Although the process is not complete yet, ICANN's agenda also includes efforts to define a special category of famous names and exclude them from the DNS database. Global exclusions of names constitute a very strong form of protection that did not exist prior to ICANN. In short, ICANN makes the entire process of domain name registration a firewall for trademark protection. Such a linkage dramatically increased the power and efficiency of trademark enforcement. It also expanded the scope of trademark protection beyond existing national laws.

By linking resource assignment to policy, the intellectual property interests followed a precedent long established in broadcasting. The foundation of broadcast regulation has always been governmental control of access to an essential resource, the radio frequency spectrum. While governments generally legitimize their control of the spectrum based on the need to eliminate electromagnetic interference via central coordination of frequency use, in actual practice control of the frequency resource is leveraged to exert power over forms of conduct entirely unrelated to electromagnetic interference, such as program content and ownership. (COASE [1959]) Indeed, broadcast legal and regulatory institutions in the US originated from a process analogous to current Internet travails. A new resource was created, a new arena of appropriation emerged, and an institutional innovation that linked resource assignment to policy was born.

The precipitating cause of institutional innovation was the creation of a new resource. The process of endowment brought the principles and norms of trademark law into an arena where it had never been applied before. It was an arena where the mapping between trademark concepts and domain names was inherently uncertain, and where the different groups involved

were unable to reach consensus about what standards or rules should be used to resolve the tension. In approaching this problem, the trademark owners projected some very novel and expansive notions of trademark protection into the institutional vacuum. Other players, notably ISOC and IANA, found it to be in their self-interest to ally themselves with the trademark interests. Eventually, their initiative was harmonized with the interests of major multinational corporations, and governmental organizations in the United States and Europe.

It is clear that objective changes in relative transaction costs, by themselves, cannot explain either the process or the outcome of this case. The emergence of a market for Internet domain names did not simply “reduce” or “increase” the transaction costs of trademark holders. Rather, the trademark interests developed a subjective (and probably overly high) assessment of the value of names in cyberspace. They then sought to create institutional arrangements that would give them the expansive rights over names in cyberspace that they thought they ought to have. They discovered along the way that control of the root server database could facilitate the enforcement of a whole range of intellectual property rights, including copyright. The new institutional arrangements they proposed were designed not only to reduce their transaction costs, but also to shift many of the costs and risks involved in policing intellectual property rights onto registries and users. They were able to get away with these proposals because technology created a new, global arena for collective action in which they succeeded in obtaining a first-mover advantage.

In short, a decline in the costs of monitoring domain names can explain why trademark holders were able to identify and act against perceived threats to their property rights in cyberspace. But it cannot explain why institutional innovations occurred, nor can it explain why they were able to assert and win dramatic increases in the scope of their rights.

The success of the intellectual property owners is also a necessary part of the explanation of the other institutional innovation, ICANN. The resolution of the problem of Internet names and numbers would have been very different had there been no trademark conflict. It is noteworthy, for example, that the transfer of the address space to the regional address registries and to ICANN never generated the political controversies or institutional innovations that the domain name wars did. The economic value of numerical IP address resources is, at the very least, equal to that of domain names. There was uncertainty about who controlled the address space, just as there was in the case of domain names. What was missing was a war over the distribution of costs and benefits.

The conflict between ISOC/IANA and NSI probably could have been resolved within the United States in a straightforward manner through the creation of an independent technical coordination body to handle Internet names and numbers. It was the trademark issue that politicized the problem and motivated ISOC and IANA to seek allies among international organizations. The US easily rebuffed the attempt of the ITU to get involved, but the strong political influence of major intellectual property and e-commerce interests, most of whom are based in the US, could not be dismissed so lightly.

## D. References

- BURK, D. [1995], "Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks," *Richmond Journal of Law and Technology*, 1, 1.
- BUSH, P. [1987], "The Theory of Institutional Change," *Journal of Economic Issues*, 21, 3, 1075-1116.
- COASE, R. [1960], "The Problem of Social Cost," *Journal of Law and Economics*, 3, 1, 1-44.
- COASE, R. [1959], "The Federal Communications Commission," *Journal of Law and Economics* 2 (October), 1.
- COASE, R. [1937], "The Nature of the Firm," *Economica*, 4, 386-405.
- DEMSETZ, H. [1964] "The Exchange and Enforcement of Property Rights," *Journal of Law and Economics* 7, 11-26.
- DEMSETZ, H. [1966], "Some Aspects of Property Rights," *Journal of Law and Economics* 9, 61-70.
- DEMSETZ, H. [1967], "Toward a Theory of Property Rights," *American Economic Review, Papers and Proceedings* 57, 347-59.
- DEPARTMENT OF COMMERCE, NTIA [1998], "Management of Internet Names and Addresses: Statement of Policy," Federal Register 63, 111 (June 10) 31741.
- DIAMOND, D. [1998], "Whose Internet Is It, Anyway?" *Wired Magazine* 6, 4 (April).
- DOMAINZ, [1998], "High Court Endorses Domainz Process," (News Release) 13 November, <http://www.domainz.net.nz/newsstand/stories/court4.html>, visited August 1999.
- FROOMKIN, A. M. [1999], "A Commentary on WIPO's The Management of Internet Names and Addresses: Intellectual Property Issues," <http://www.law.tm/>, visited August 1999.
- FUROBOTN, E. AND R. RICHTER [1998] *Institutions and economic theory: The contribution of the new institutional economics*. University of Michigan Press: Ann Arbor, MI.
- HAZLETT, T. [1990], "The Rationality of US Regulation of the Broadcast Spectrum," *Journal of Law and Economics*, 33, 133 - 175.
- IAHC (International Ad Hoc Committee) [1997] Final Report <http://www.iahc.org/draft-iahc-recommend-00.html> visited May 1999.
- INTA (International Trademark Association) [1998], "Board the Moving Bus: Trademark Owners Beware of Proposals to Improve Management of Internet Names and Addresses," *Trademark Reporter*, May-June.
- LIBECAP, G.D. [1989] "Distributional Issues in Contracting for Property Rights," *Journal of Institutional and Theoretical Economics* 145, 6-24.
- Lockheed Martin Corp v Network Solutions, Inc*, 985 F Supp 949, 951 (CD Cal 1997)
- MINASIAN, J. [1970], "The Political Economy of Broadcasting in the 1920s," *Journal of Law and Economics* 12, 2, 391.

- MOCKAPETRIS, P. [1987] "Domain names: Concepts and Facilities," Internet Society, RFC 1034 (November).
- MOSKIN, J.E. [1998], "Domain Name 'Reforms' Will Inflamm Internet Problems," *IP Worldwide*, (July/August).
- MUELLER, M. [1998], "The battle over Internet domain names: global or national TLDs?" *Telecommunications Policy*, 22, 2, 89-108.
- MUELLER, M. [1999], "Trademarks and Domain Names: Property Rights and Institutional Evolution in Cyberspace." *Selected Papers from the 1998 Telecommunications Policy Research Conference*, S. E. Gillett. and I. Vogelsang, eds., LEA, Mahwah, New Jersey.
- NATHENSON, I. S. [1997], "Showdown at the Domain Name Corral: Property rights and personal jurisdiction over squatters, poachers, and other parasites." *University of Pittsburgh Law Review*, 58, 994.
- NORTH, D.C. [1990] *Institutions, Institutional Change, and Economic Performance*, Cambridge University Press: Cambridge.
- NORTH, D.C. [1993] "Institutional Change: A framework of analysis" in Sjostrand, S.J., (ed.) *Institutional Change: Theory and Empirical Findings*, M.E. Sharpe: Armonk, NY.
- OSTROM, E. [1990]. *Governing the Commons*, Cambridge University Press: Cambridge.
- OPPEDAHL, C. [1999], "Recent trademark cases examine reverse domain name hijacking," *Hastings Comm/Ent Law Journal*, 21, 535.
- Panavision International v. Toeppen*, No. 97-55467, slip op. (9<sup>th</sup> Cir. April 17, 1998).
- PGMedia, Inc. d/b/a Name.Space v. Network Solutions, Inc., et al.*, Order, S.D.N.Y., 97 Civ. 1946 (RPP), 1999 U.S. Dist. Lexis 2997 (March 17, 1999)
- POST, D. [1998], "Cyberspace's Constitutional Moment," *American Lawyer* (November), 117.
- POSTEL, J. [1994], "Domain Name System Structure and Delegation," Internet Society, *RFC 1591* (March).
- RONY, E and RONY, P. [1998], *The Domain Name Handbook*, R&D Publications: Lawrence, KS.
- RUTHERFORD, M. [1994], *Institutions in Economics: The old and the new institutionalism*, Cambridge University Press: Cambridge.
- RUTKOWSKI, A.M. [1998] "Internet DNS Historical Timeline," at <http://www.wia.org/dns-law/pub/timeline.html>, visited August 1999.
- RUTTAN, V. AND Y. HAYAMI [1984] "Toward a Theory of Induced Institutional Innovation," University of Minnesota Working Papers, 200 (February).
- SIMON, C. [1998] "The Technical Construction of Globalism: Internet Governance and the DNS Crisis," unpublished ms., <http://www.flywheel.com/ircw/dnsdraft.html> visited August 1999.

SJOSTRAND, S. (Ed.), [1993], *Institutional Change: Theory and Empirical Findings*, M.E. Sharpe: Armonk, NY.

SU, Z. and POSTEL, J. [1982], "The Domain Naming Convention for Internet User Applications," Internet Society, RFC 819 (August).

WIPO [1998], "The Management of Internet Names and Addresses: Intellectual Property Issues." (Interim Report, December) World Intellectual Property Organization: Geneva.

WIPO [1999], "The Management of Internet Names and Addresses: Intellectual Property Issues," (Final Report, April) World Intellectual Property Organization: Geneva.