ICANN May Be the Only Game in Town, But Marina del Rey Isn't the Only Town on Earth: Some Thoughts on the So-Called "Uniqueness" of the Internet

by
*Volker Kitz**

I. INTRODUCTION

"If you want to attach your network to the Internet, but you don't like the Network Solution, Inc.'s[1] ("NSI") policies, for whatever reason, you quickly learn that NSI is the only game in town," said Catherine Simmons-Gill at a Congressional hearing in 1996.[2] One might pose the question, "Why not just go to a different town?" Unfortunately, no other "town" can pride itself on hosting an organization that ultimately presides over the assignment of domain names under the current domain name system. The Internet Corporation for Assigned Names and Numbers ("ICANN"), based in Marina del Rey, is presently in charge of domain name administration and is unparalleled in its authority. It has long been claimed that the "uniqueness" of domain names and of the Internet effectively prohibits competition for ICANN.

This article argues that this is an incorrect assumption and that the world need not depend on ICANN as it presently does. First, the current domain name system ("DNS") will be briefly explained and then its inherent difficulties explicated. The article will then compare the system to traditional concepts of global communication and explain why cyberspace can and should adopt telecommunications as a model. Finally, it will explore an alternative system in which ICANN would lose its unparalleled status.

---

* LL.M., New York University; Hauser Global Scholar 2001-2002; Assistant Researcher, Universitaet zu Köln, Cologne, Germany (Professor Dr. Barbara Dauner-Lieb). The author wishes to thank Professor Norman Dorsen, Professor Dr. Matthias Herdegen, and the Hauser Global Scholars 2001-2002 for comments on earlier drafts.

1. *See* discussion *infra* Parts III.B and III.D (Network Solution Inc. ("NSI"), is the predecessor of the Internet Corporation for Assigned Names and Numbers ("ICANN") in administering the assignment of domain names. ICANN is currently in charge of domain name administration. NSI was subsequently acquired by VeriSign, Inc., which still operates the .com and .net top level domain registries pursuant to agreements with ICANN and the United States government.

2. *Copyright Protection on the Internet: Hearings Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary on H.R. 2441*, 104th Cong., 2d Sess. (1996) (statement of Catherine Simmons-Gill on behalf of the International Trademark Association).

II. The Current Domain Name System

A. How the Domain Name System Works

Internet traffic is fairly simple. It involves communication between two computers: one user enters a certain domain name into her browser software and then retrieves a website hosted[3] by another computer.[4] The other computer may be located next door or thousands of miles away. Theoretically, the first computer "calls" the second computer to retrieve content data for the desired website. The crucial information that the first computer requires to accomplish this "call" is the identity and location of the second computer. In other words, if a user types "www.microsoft.com" into a browser, the computer must identify the computer that holds the content data for the website "www.microsoft.com," which will finally be displayed on the screen of the calling computer.

In order to facilitate the communication between two given computers in the world, every computer on the Internet is identified through a numbering scheme. It designates the location of every computer on the network by allocating the computer an Internet Protocol ("IP") number.[5] Merely consisting of strings of numbers,[6] IP addresses are not very helpful for memorable website identification and have proven awkward for users to handle. So, for easier access, these numbers are matched with an alphanumeric domain name.[7] The complete alphanumeric domain name is constructed in two parts. One part of the name consists of a top-level domain ("TLD") that represents either an individual country (*e.g.* jp = Japan) or a generic grouping ("gTLDs") (*i.e.*, .com, .gov, .edu, .net, .org, and .mil). The second component is a second level domain name that appears left of the gTLD in the address line. The second level domain name provides the specific name of the entity (*e.g.*, "microsoft" in microsoft.com).[8]

Lists of valid IP numbers and their matching domain names or aliases are maintained in a series of computers called "name servers." These name servers hold a directory for individual computers seeking the location of an address contained in the database. An individual computer will query the

3. "Hosting" means storage of the content data of a website.

4. The content data of a specific website is stored on the hard disk of the hosting computer. Every website has a physical storage location; thus it is inaccurate to call the Internet "intangible."

5. *See* Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 10, 1998) [hereinafter White Paper].

6. In the format of "120.34.26.192," for instance.

7. For example, instead of having to use 192.0.34.65, a user can use www.icann.org. This is especially helpful since e-mail addresses use domain names.

8. Stuart D. Levi et al., *The Domain Name System & Trademarks*, 563 PLI/PAT 449, 485-86 (1999).

directory with the domain name that was entered by the user, such as "www.microsoft.com."[9] The name server then matches "www.microsoft.com" with its associated IP number, and, in a second step, directs the user to the individual computer that is assigned to this specific IP number.[10]

Not every name server contains information about all existing domain names, however. Instead, each TLD has an "authoritative" name server with the directory for that specific TLD.[11] Therefore, queries must be directed to the correct name server in order to resolve a given domain name successfully.[12] The necessary guidance is provided by root name servers, which contain the addressing information for all the authoritative TLD name servers.[13] As a consequence, a root name server is the central and critical part in resolving a domain name. Without the root name server, no computer could find its way through the Internet, much less be able to retrieve a single website.

B. Who Controls the Domain Name Servers?

Since the DNS depends entirely upon the root name server, the entity that controls the root name server also controls the DNS, and thus it can also be said to control the entire operation of the Internet.[14] Currently, there are thirteen root name servers worldwide, ten of which are located in the United States, one in Stockholm, one in London/Amsterdam, and one in Tokyo.[15] The Internet's most important infrastructure is not completely centralized in any one location and is beginning to be "dispersed globally."[16] Among the

9. *See* InterNIC, *The Domain Name System: A Non-Technical Explanation*, *available at* http://www.internic.net/faqs/authoritative-dns.html (last visited Feb. 15, 2004) (explaining that translation of the IP name into the IP address is called "resolving the domain name").

10. Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 554 (1998) ("If your name is on the list, you can be found on the Internet. If not, anyone who types that name into their browser or mail program will not be able to reach you.").

11. *Id.*

12. *Id.*

13. Levi et al., *supra* note 8, at 453 (noting that for reasons of performance, "name resolvers" routinely download and copy the information contained in the root servers and can then be directly addressed by users).

14. A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 166 (2000) (noting that the entity in control of the "root name server" can also control changes in the Internet's architecture and therefore "govern" the Internet).

15. Overview of Servers, *available at* http://www.root-servers.org (last visited Feb. 15, 2004).

16. Shamoil Shipchandler, Note, *The Wild Wild Web: Non-Regulation as the Answer to the Regulatory Question*, 33 CORNELL INT'L L.J. 435, 437 (2000).

thirteen root name servers, the so-called "A" root server, located in Dulles, Virginia, is the most important one. It is, in fact, the ultimate authority in the DNS hierarchy, regularly duplicating and transmitting its data to the other twelve root servers and constantly ensuring that all thirteen root name servers contain the same information. In this system, the other twelve root name servers merely serve as backups to meet the demands of heavy Internet traffic, essentially acting as nothing more than "operational satellites" to the "A" root server.

The question then becomes, who controls the crucial "A" root server? Between 1993 and 1999, NSI was in charge of the DNS management under a contract with the U.S. Government.[17] On July 1, 1997, as a part of the Clinton Administration's *Framework for Global Electronic Commerce*,[18] the President directed the Secretary of Commerce to privatize the DNS to increase competition and facilitate international participation.[19] Subsequently, the National Telecommunications and Information Administration ("NTIA"), an agency of the Department of Commerce, issued for comment a rulemaking proposal known as the "Green Paper."[20] The "Green Paper" proposed a

17. A brief history of the DNS can be found in the White Paper, *supra* note 5: In the early 1970s, the U.S. Government began funding research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of Defense's Advanced Research Projects Agency ("DARPA"). ARPANET was later linked to other networks established by other government agencies, universities and research facilities. During the 1970s, DARPA also funded the development of a "network of networks"; this became known as the Internet, and the protocols that allowed the networks to intercommunicate became known as Internet protocols. Dr. Jon Postel, then a graduate student at the University of California at Los Angeles, undertook the maintenance of a list of host names and addresses under contracts with DARPA. Beginning in 1987, IBM, MCI and Merit developed NSFNET, a national high-speed network based on Internet protocols, under an award from the National Science Foundation ("NSF"). On December 31, 1992, NSF entered into a cooperative agreement with Network Solutions, Inc. under which NSI would provide the domain name registration services. Subsequently, NSI managed key registration, coordination, and maintenance functions of the DNS. In 1992, the U.S. Congress gave NSF statutory authority to allow commercial activity on the NSFNET. *See* Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(a) (2000). The Internet has thus evolved from the stages of a military tool and a scientific network to a commercial application.

18. U.S. Dep't of Commerce, *Framework for Global Electronic Commerce, available at* http://www.ecommerce.gov (on file with the author).

19. President William J. Clinton, Remarks by the President in Announcement of Electronic Commerce Inititive, *available at* 1997 WL 362676 (July 1, 1997) [hereinafter Presidential Directive].

20. Improvement of the Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8825 (Feb. 20, 1998) [hereinafter Green Paper].

private sector creation of a new not-for-profit corporation managed by a globally and functionally representative Board of Directors. The "Green Paper" was followed by a more elaborate "White Paper," under which a new private entity would assume responsibility for the coordination of the protocol number assignment, the management of the root name server system, the creation of new TLDs, and the assignment of technical parameters as needed to maintain universal connectivity on the Internet.[21]

Accordingly, the ICANN was created. ICANN is a self-funded, not-for-profit California corporation organized without members.[22] ICANN entered into an agreement[23] with the United States Department of Commerce called the Memorandum of Understanding ("MOU"), under which ICANN assumed responsibility for coordinating the stable operation of the Internet in four key areas: (1) the DNS, which ICANN oversees through the Internet Assigned Numbers Authority ("IANA"), an entity under ICANN's control; (2) the allocation of IP address space; (3) the management of the root server system; and (4) the coordination of the protocol number assignment.

ICANN-accredited registrars administer the registration of all second level domain names under the traditional gTLDs, such as .com, .edu, .org, and .net, as well as under the newly created gTLDs.[24] Administration of the national TLDs (called "country code" TLDs, and abbreviated as ccTLDs)[25] generally lies in the hands of entities within each country under agreements with ICANN. Only if ICANN includes the ccTLDs and the gTLDs in the "A" root server list are web addresses containing these ccTLDs and gTLDs

21. *See* White Paper, *supra* note 5.

22. *See* ICANN, *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*, *available at* http://www.icann.org/general/articles.htm (last visited Feb. 15, 2004) [hereinafter ICANN, *Articles of Incorporation*]; *see also* ICANN, *Bylaws for Internet Corporation for Assigned Names and Numbers*, *available at* http://www.icann.org/general/bylaws.htm (last visited Feb. 15, 2004) [hereinafter ICANN, *Bylaws*].

23. ICANN, *Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation of Assigned Names and Numbers*, *available at* http://www.icann.org/general/icann-mou-25nov98.htm (Nov. 25, 1998) [hereinafter ICANN, *Memorandum of Understanding*].

24. *See* ICANN, *Accredited Registrars*, *available at* http://www.icann.org/registrars/accredited-list.html (last visited Feb. 15, 2004). Seven new TLDs were selected by ICANN in November 2000 to be included in the DNS: .biz, .info, .pro, .name, .coop, .aero, and .museum. *See* ICANN, *Top-level Domains, available at* http://www.icann.org/tlds (last visited Feb. 15, 2004).

25. Country code TLDs are two letter codes such as ".jp" for Japan. *See, e.g.,* Internet Assigned Number Authority, *Root-Zone WhoIs Information*, *available at* http://www.iana.org/cctld/cctld-whois.htm (last visited Feb. 15, 2004) (listing the two letter abbreviations used for several countries).

accessible to users elsewhere on the Internet.[26] Consequently, one could strongly argue that ICANN ultimately controls the current DNS.

III. Problems Under the Current Regime

Due to the centralization and non-competitive nature of the current domain name system, the current regime faces a variety of severe problems.

A. Scarcity of Domain Names

One of the major disadvantages inherent to the current system is the scarcity of domain names.[27] Practically all relatively short generic second level domain names under the valuable gTLDs have already been assigned to individuals or entities and are "off the market." Further, the fact that the only gTLD that has any significance in the public's mind is the ".com" extension makes the scarcity of domain names even more critical.[28] Coming up with an imaginative, artificial name has become a key factor for new businesses wanting to participate in Internet commerce. For example, if World Travel Partners, based in Atlanta, Georgia, is the registered owner of the domain "travelagent.com," every other travel agent in the world must find a different and less descriptive name for Internet activity and might eventually be forced to resort to calling itself something like "travelocity.com." Moreover, it is of little help to an Internet user in Sweden to find an Atlanta based travel agent at "travelagent.com." It is this scarcity of domain names that has given rise to a plethora of trademark related disputes.

B. Lack of Transparency in Decision Making

Where scarcity of resources such as domain names exists, transparency in allocating the resources becomes of paramount importance. ICANN's selection process for the new gTLDs has been criticized precisely for its lack of transparency. Representative Edward Markey noted that the "[d]ecisions made in the Vatican to select the Pope are more clear to the public than how new domain names are issued" and that "only a small high priesthood of the

26. Lemley & McGowan, *supra* note 10, at 554 n.321 (explaining that "If the root DNS name servers are not configured to "recognize" a TLD (like ".web"), they simply will not match it with an IP address, and messages to that domain will not be delivered. Period.").

27. *See* Joseph P. Liu, *Legitimacy and Authority in Internet Coordination: A Domain Name Case Study*, 74 Ind. L.J. 587, 604 (1999).

28. David P. Collins, Note, *Internet Ambush, Using the Patent and Trademark Office to Shut Down a Competitor's Domain Name*, 4 Chap. L. Rev. 231, 253 (2001).

Internet fully understands how these decisions are made."[29] The selection process appears to be random rather than predictable.[30]

As long as ICANN's legal nature and its authoritative actions, if there are any at all,[31] remain unclear, its decisions will always lack transparency.[32] The Memorandum of Understanding that governs ICANN refers to ICANN's own Articles of Incorporation[33] and Bylaws[34] as providing authority for ICANN's control of the DNS project.[35] Of course, this is nothing more than a circular reference to self-given authority.[36]

C. Traffic Overflow and the "Internet II Project"

With the number of Internet users growing exponentially,[37] capacity limits become more noticeable. Internet traffic has become slow because the technical infrastructure is swamped with too many requests from all over the

29. Anthony Shadid, *The Name Game*, BOSTON GLOBE, April 9, 2001, at C1.

30. The lack of transparency in the introduction of the new .biz TLD has prompted a First Amendment complaint against ICANN. *See* Smiley v. ICANN, No. BC-254659, slip op. at 9 (Cal. Super. Ct., Aug. 1, 2001) (alleging that the introduction process involves a "illegal lottery enterprise"). A collection of documents in this case is accessible via the Internet. *See* ICANN, *Litigation Documents*, *available at* http://www.icann.org/legal/litigation.htm (last visited Feb. 15, 2004).

31. *See* KLAUS W. GREWLICH, GOVERNANCE IN "CYBERSPACE": ACCESS AND PUBLIC INTEREST IN GLOBAL COMMUNICATIONS 56 (1999) (noting that ICANN's legal authority has not been established up to the present day); *see also* Volker Röben, *International Internet Governance*, 42 GERMAN Y.B. OF INT'L LAW 400, 415 (2000); Lemley & McGowan, *supra* note 10, at 554 (stating the same issue existed under NSI, "NSI is a private entity; it is not at all clear what authority it has to "run" the Internet, or indeed who might be able to give it that authority").

32. *See* Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You – Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89, 177 (2001) (noting that because ICANN is not a governmental organization, it is not subject to "openness" laws, such as the Sunshine Act or the Freedom of Information Act, to ensure transparency in decision making).

33. ICANN, *Articles of Incorporation*, *supra* note 22.

34. ICANN, *Bylaws*, *supra* note 22.

35. *See* ICANN, *Memorandum of Understanding*, *supra* note 23; *see also infra* Part III.D (acknowledging the authority of the Department of Commerce to participate in the DNS Project).

36. *See* ICANN, *Background*, *available at* http://www.icann.org/general/background.htm (last visited Feb. 15, 2004) (ICANN itself concedes that it "has no statutory or other governmental power").

37. Russell B. Stephenson, *Internet Payment Systems and the Cybercash Approach*, 452 PLI/PAT 123, 126 (1996).

world.[38] Thirteen root name servers handle millions of domain name resolutions every day, using the important "backbones" to send their data to different users spread over different countries and continents. As a consequence, collaborative efforts are already being made among a number of universities, federal research and development agencies, and private sector firms to develop a next generation Internet, called the "Internet II."[39]

D. Insufficient Participation of Countries Outside the United States

Internet users outside the United States have objected to the current system because it concentrates authority over the DNS in the hands of the United States.[40] In fact, every individual user, as well as the national registrars, is fully at ICANN's "mercy." If ICANN refuses to enter a certain domain name into the root name server database, that domain name cannot be assigned to an individual.

No other country influences the assignment of the valuable gTLDs. "Every other country in the world has to settle for their two-letter International Organization for Standardization code. The United States gets to sit on and allocate a whole bunch more than that."[41] The gTLDs ".gov, .mil, and .edu" are reserved for exclusive use by United States registrants. Moreover, if ICANN decides to exclude a national TLD from its database, the affected country will no longer have its "virtual territory" on the Internet. On the Internet, the country virtually ceases to exist. Finally, if ICANN decides to shut the entire root server system down, the Internet will be immediately effectively closed to the world.

In spite of these concerns, ICANN remains under strong American influence. Although the White Paper concluded in 1998 that "[a]n increasing percentage of Internet users reside outside of the U.S.,"[42] the controlling entity ICANN still operates under a private agreement with the U.S. Department of Commerce.[43] While the official purpose of this agreement is the privatization of the DNS, the agreement makes it clear that "the Parties will

38. *See* Internet II & UCNET, *The Internet II Project: General Information*, *at* http://www.id.ucsb.edu/detche/library/www/internet2.html (last visited Feb. 15, 2004) (stating that the frequent congestion has "deprived many faculty of the network capability needed to support world class research").

39. *Id.*

40. Röben, *supra* note 31, at 413 (referencing *Corporations, Governments, Agencies, Individuals from all over the World Find Major Flaws in U.S. Green Paper*, *at* http://www.gtld-mou.org/press/core-7.html (last visited Feb. 15, 2004)).

41. David Diamond, *Whose Internet Is It, Anyway?*, WIRED MAGAZINE, *at* http://www.wired.com/wired/archive/6.04/kashpureff.html (last visited Feb. 15, 2004) (quoting Eugene Kashpureff).

42. *See* White Paper, *supra* note 5.

43. *See* ICANN, *Memorandum of Understanding*, *supra* note 23.

collaborate on the DNS Project" and "will jointly design, develop, and test the mechanisms, methods, and procedures."[44] The responsibilities of the Department of Commerce under the agreement specifically include "[m]aintain[ing] oversight of the technical management of the DNS functions."[45] In contrast, the description of ICANN's responsibilities, as revised by Amendment 6, entered on September 17, 2003,[46] still consists mostly of limited activities such as providing expertise, working collaboratively, developing, testing, and implementing as well as consulting.[47]

Therefore, it may be appropriate to say that the U.S. Department of Commerce controls ICANN, and that ICANN's role is limited to mere collaboration. In Amendment 3 of the Memorandum, the Department of Commerce ensured its continued control over the DNS even in the event that ICANN ceases to operate.[48] Amendment 5[49] implemented obligatory annual reports to the Department. Recently, in September 2003, the term of the Memorandum was extended until September 30, 2006, while the parties recognized that "the technical management of the Internet and its underlying domain name system (DNS) [is] now performed by or on behalf of the U.S. Government or by third parties under arrangements or agreements with the U.S. Government."[50]

---

44. ICANN, *Memorandum of Understanding*, *supra* note 23, at art. II.B. (quoting the "Purpose").

45. ICANN, *Memorandum of Understanding*, *supra* note 23, at art. V.B. (quoting the "Responsibilities of the Parties").

46. ICANN, *Amendment 6 to Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation of Assigned Names and Numbers*, *available at* http://www.icann.org/general/amend6-jpamou-17sep03.htm (Sept. 19, 2003) [hereinafter *Amendment 6*].

47. ICANN, *Memorandum of Understanding*, *supra* note 23 (In the original version of the memorandum, almost all the descriptions of ICANN's responsibilities began with the word "collaborate.").

48. ICANN, *Amendment 3 to Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation of Assigned Names and Numbers, available at* http://www.icann.org/general/amend3-jpamou-25may01.htm (May, 25, 2001) (stating that "If the Department of Commerce withdraws its recognition of ICANN or any successor entity by terminating this Memorandum of Understanding, ICANN agrees that it will assign to the Department of Commerce any rights that ICANN has in all existing contracts with the registries and registrars").

49. ICANN, *Amendment 5 to Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation of Assigned Names and Numbers, available at* http://www.icann.org/general/amend5-jpamou-19sep02.htm (Sept. 19, 2002).

50. *See* ICANN, *Amendment 6*, *supra* note 46.

The U.S. Department of Commerce assumes authority for its participation in the DNS Project under several national statutes,[51] a presidential memorandum,[52] and a self-issued statement of policy.[53] Because the U.S. Government has retained a high degree of control over the DNS, internal ICANN decisions are of limited relevance. Foreign countries, however, do not have an adequate influence on these internal proceedings. According to Article VI of its Bylaws, ICANN's general powers are vested with a Board of Directors.[54] While it is true that Article VI, Section 5 of the Bylaws seeks to implement a minimum of regional diversification,[55] this does not involve other countries as governments in the decision making process. Such a view is supported by Article VI, Section 7, which hastens to clarify that "[d]irectors shall serve as individuals . . . and not as representatives of . . . any other organizations or constituencies."[56] Similarly, the "Governmental Advisory Committee," provided for in Article XI, Section 2(1) of the Bylaws, is not much more than a cosmetic effort to make ICANN appear international. Membership in the Advisory Committee is open to all national governments and, upon the invitation of the Committee itself or of the ICANN Board, to "Distinct Economies as recognized in international fora,

51. *See* 15 U.S.C. § 1525 (2000) (authorizing joint projects); 15 U.S.C. § 1512 (2000) (authorizing, fostering, promoting and developing domestic commerce); 47 U.S.C. § 902 (2000) (authorizing of the National Telecommunications and Information Administration to coordinate telecommunications activities of the Executive Branch).

52. *See* Presidential Directive, *supra* note 19 (directing the Secretary of Commerce to transition the DNS management to the private sector).

53. *See* White Paper, *supra* note 5 (Attachment A) (describing the manner in which the Dep't of Commerce will transition DNS management to the private sector).

54. *See* ICANN, *Bylaws*, *supra* note 22, at art. VI.

55. *See* ICANN, *Bylaws*, *supra* note 22, at art. VI § 5. The Bylaws state:

> In order to ensure broad international representation on the Board, the selection of Directors by the Nominating Committee and each Supporting Organization shall comply with all applicable diversity provisions of these Bylaws or of any Memorandum of Understanding referred to in these Bylaws concerning the Supporting Organization. One intent of these diversity provisions is to ensure that at all times each Geographic Region shall have at least one Director, and at all times no region shall have more than five Directors on the Board (not including the President). As used in these Bylaws, each of the following is considered to be a ''Geographic Region': Europe; Asia/Australia/Pacific; Latin America/Caribbean islands; Africa; and North America. The specific countries included in each Geographic Region shall be determined by the Board, and this Section shall be reviewed by the Board from time to time (but at least every three years) to determine whether any change is appropriate, taking account of the evolution of the Internet.

56. ICANN, *Bylaws*, *supra* note 22, at art. VI § 7.

and multinational governmental organizations and treaty organizations."[57] The Governmental Advisory Committee, however, has no actual influence on the decision making process. Its activities are limited to providing "advice on the activities of [the Corporation] as they relate to concerns of governments."[58] Interestingly, ICANN, whose own legal authority is in doubt, does not hesitate to make it clear that "Advisory Committees shall have no legal authority to act for ICANN, but shall report their findings and recommendations to the Board."[59]

IV. Paradigms of Communication Regulation

In evaluating the criticism that the current DNS is facing, one ought to consider how governments regulate other areas of worldwide communication. Both the telephone system and the postal system exhibit a global communication structure that has produced specific legislation and governing bodies under international law. Much can be learned from these traditional forms of global networks.

A. The Telephone System

In light of the so-called "vanity numbers,"[60] the telephone numbering system especially lends itself to a comparison with the domain name system.[61]

1. The Problems of the Domain Name System do not Exist

The comparison shows that the traditional telephone system does not produce the same difficulties and criticisms as the domain name system. Originally faced by the same problems inherent in every global communication network, the international telephone system has, unlike the DNS, found ways of dealing with these problems.

a. Every Country Controls its Own Territory

The first apparent difference between the DNS and the telephone numbering system is that responsibility for the latter lies in the hands of each country with respect to its own territory. The registration of telephone numbers is perceived as an exclusive right of each national government. No country feels subjected to the decisions of foreign entities because it retains

57. ICANN, *Bylaws*, *supra* note 22, at art. XI § 2.

58. ICANN, *Bylaws*, *supra* note 22, at art. XI § 2.

59. ICANN, *Bylaws*, *supra* note 22, at art. XI § 1.

60. Vanity numbers are expressed in letters rather than in digits, for instance 1-800-TRAVELAGENT.

61. *See* Shipchandler, *supra* note 16, at 450; *see also* Grewlich, *supra* note 31, at 33 (stating that the Internet has characteristics of the telephone, telegraph, television, and radio and is both a conversational and a mass medium).

control over the assignment of all telephone numbers within its country code at all times. Even more importantly, the technical infrastructure for the routing of all calls directed to national numbers physically lies within national boundaries. Hence, each country not only has a legal, but also an actual physical control over the assignment routing of all national telephone numbers. This control is inherently very different from the pseudo-control of the kind implemented via ICANN's subsidiaries.[62]

b. Transparent Decisions

Since national law governs the assignment of telephone numbers,[63] the process is transparent, predictable, and subject to judicial review. Unlike the ambiguity surrounding ICANN, the legal authority for the national agencies to act as registrars for telephone numbers is clear, as are the rules governing their acts.[64]

c. Less Scarcity

Scarcity is, naturally, also an issue with the telephone numbering system. As populations increase and more telephone users emerge, countries face exhaustion of their original numbering resources. Where "only" numbers are concerned, this is not a problem; the numbers simply get longer. The resources are more limited, however, when it comes to "vanity numbers." The number 0800-DOCMORRIS, for instance, can only be assigned once in each country. Although scarcity is not as extreme as with the DNS—where www.0800docmorris.com cannot be assigned in each country under the current DNS, but only to one single owner worldwide—the resources obviously cannot meet the demand for specific letter combinations. Vanity numbers also work with area codes, however, so that the local number (area code) DOCMORRIS can be assigned to as many telephone users as there are area codes. Since each country is free to create new area codes and even new codes for national telephone services like 0800, each country has the means to deal with its own scarcity without depending upon a foreign-based entity like ICANN.

d. Less Traffic Overflow

Finally, since every country has its own routing infrastructure, traffic overflow is not nearly as serious a problem as it is on the Internet. Whereas the infrastructure at the "heart" of the Internet constantly has to handle the entire traffic worldwide, the national telephone system routers only have to deal with traffic originating from or directed to a national telephone user. All

62. *See supra* Part III.D.

63. GREWLICH, *supra* note 31, at 36; *see also* Telecommunications Act, § 43 17 Dec. 1997 (Federal Law Gazette I 3108) (German Telecommunication Act).

64. *See, e.g.*, § 66 TKG (establishing the authority for the Regulierungsbehörde für Telekommuniaktion und Post).

countries share in the power to control the system, but they also share in the burden of handling it.

2. Decentralization as the Reason

It is apparent from the foregoing discussion that decentralization is the main factor allowing the telephone system to avoid the problems currently facing the DNS. Given the fact that the worldwide telephone system consists of many autonomous national telephone networks, the main problem shifts and is limited to one fairly easy-to-handle issue, the issue of interconnection, which is "at the heart of the phone system."[65] Since the issue of interoperability has been resolved by the global telephone system, an endless number of autonomous national networks can participate in one global network. The telephone system, therefore, is the paradigmatic example of a "pure" network.[66]

For the global telephone network, interoperability is ensured under the auspices of the International Telecommunication Union ("ITU"). The ITU accomplishes this task by developing and setting the necessary technical standards. Being a specialized agency within the regime of the United Nations, neither its legal authority nor the transparency of its decisions is in serious doubt.

B. The Postal System

With methods similar to those utilized by the telephone system, the global postal system also avoids the specific problems faced by the DNS. The postal system is decentralized; each country is in charge of assigning postal codes, street names, and numbers (the latter two being even more decentralized through the engagement of local rather than federal agencies). Thus, as with the telephone system, decentralization in the postal system yields positive results: (1) control of each country over its own territory; (2) transparent, predictable decisions on the basis of national law; (3) practically no scarcity;[67] and (4) no overflow problems. In this system, interoperability of the national postal networks is ensured by the Universal Postal Union ("UPU"), another specialized agency within the regime of the United Nations.

---

65. Lewis Katz & Jay Shapiro, *Network Externalities, Competition and Compatibility*, 75 AM. ECON. REV. 424, 424 (1985) ("In a network, the 'utility that a user derives from consumption of a good increases with the number of agents consuming the good.' "); *see also* Lemley & McGowan, *supra* note 10, at 546 ("We are all better off connected to the same phone network than we would be connected to different phone networks.").

66. Lemley & McGowan, *supra* note 10, at 546 ("It is no surprise, therefore, that the efficient number of telephone networks worldwide is one.").

67. There is little scarcity in distribution of addresses because addresses can be duplicated outside of particular sorting districts or zip codes.

V. "UNIQUENESS" AS A PHANTOM OBSTACLE IN CHANGING THE CURRENT REGIME

Given the rather smooth operation of the international telephone system and the global postal system, the question arises as to why the DNS—another global network of networks—has developed in such a different manner.[68] Apparently, the "traditional" concepts of global communication have not served as models for the DNS. Despite all the difficulties and the heavy criticism the DNS is currently facing, no serious efforts are being made to adapt the long-proven structures of the telephone or the postal system to the DNS.

A. The Alleged Uniqueness of Domain Names

The justification commonly referred to in support of maintaining the *status quo* involves the uniqueness of the DNS and of the Internet itself. Traditional regulatory approaches, it is argued, cannot be applied to the Internet.[69] The Internet allegedly differs from the telephone system in that it has "no physical presence" and is "located nowhere."[70] It has thus been referred to as an "invisible, intangible world of electronic information and processes."[71] The Internet is understood to be "linked together by a globally unique address space"[72] where "computer addresses need to be allotted globally according to a uniform system [that] constitutes a scarce resource since a given address can be allotted within the system only once."[73] Because of this uniqueness, some argue that there is no alternative to the centralized DNS

68. Röben, *supra* note 31, at 404 ("Given the experience with the telephone network and its parallels with the Internet, one might expect the latter to exhibit the same market structure.").

69. Shipchandler, *supra* note 16, at 450 ("The Internet's unique technology renders nations' regulations modelled after satellite and telephone technology inapplicable and ineffective."). It must be conceded that the technology of packet-switching does make the Internet unique insofar as content control is concerned. The packet-switching makes it more difficult to perform border-controls on the Internet than with other terrestrial wire-based or microwave-based technologies. *See also* GREWLICH, *supra* note 31, at 33. However, regulation on the content level and on the operational level are two different issues.

70. Shipchandler, *supra* note 16, at 436 (stating that "cyberspace is a vacuum that abhors regulation").

71. *Compare* ACLU v. Reno, 929 F. Supp. 824, 830-31 (E.D. Pa. 1996) (noting that it is only a psychological effect that makes users think of themselves as being on the global medium Internet itself rather than being connected to a private computer networking group), *with* GREWLICH, *supra* note 31, at 1.

72. GREWLICH, *supra* note 31, at 38.

73. Röben, *supra* note 31, at 412.

currently run by ICANN.[74] The alleged uniqueness of domain names thus becomes the crucial difference between the DNS and the global telephone or postal system. It is the very reason that prevents us from adopting the traditional and effective legal structures of global communication to cyberspace.

B. The Assumption is Wrong

The perceived "uniqueness" of the Internet has been stressed so repeatedly that it almost seems sacrilegious to express doubts regarding such assertions. These arguments do not, however, hold true upon close examination. ICANN admits that "anyone can create a root system similar to the *unique* authoritative root managed by ICANN."[75] This statement is, of course, a contradiction in itself: if anybody can do something, it is not unique.

ICANN is perfectly correct, however, with respect to the first part of the aforementioned statement because, under the DNS, each domain name is unique only as long as all Internet users consult the same root name server. There is, however, no technical reason that would require all users to do so. There can be two or more different name server directories maintained in autonomous root name servers by a number of different autonomous entities. What website a user reaches by typing "www.microsoft.com" in a browser would then depend on which of the directories, that is, which of the many root name servers, the browser consults.[76] In this respect, it is analogous to using phonebooks of different cities.

Computer expert Eugene Kashpureff vividly demonstrated that this scenario is not merely theoretical.[77] In April 1998, he started AlterNIC, an alternative root name server, consisting of eight computers across North America, running alternative domain name directories. These root name servers not

74. Even assuming that the DNS can only be run in a centralized way, that is, by one entity, the question still remains why this entity has to be ICANN, whose legal authority is in doubt. A centralized system can be governed by an international organization that is not controlled by the laws of a single country, but instead by its member states. In both cases, however, it is equally difficult, if not impossible, to give each country enough influence within the decision-making processes so that the Internet could rightfully be called a "global" network.

75. InterNIC, *supra* note 9 (emphasis added).

76. Neal J. Friedman & Kevin Siebert, *The Name is Not Always the Same*, 20 SEATTLE U. L. REV. 631, 663 n. 202 (1997) (stating that "[g]etting around the InterNIC monopoly is not terribly difficult. End users can simply reconfigure their desktop TCP/IP clients to use an alternative Domain Name Server (DNS) instead of their normal server. This requires more knowledge of computer programming than the vast majority of Internet users possess and it is not likely that large numbers of users would be willing to tinker with the TCP/IP settings.").

77. *See* Diamond, *supra* note 41, at 2 (discussing how Kashpureff opposed the "lack of choice . . . the fact that the control of domain-name space still lies with the US government").

only supported new TLDs, but they also remained consistent with the "traditional" TLDs. Thus, one could still get to the .com names, but in addition to those, Kashpureff added new names to the database such as .xxx, .med, .nic, .ltd, .lnx, and .exp.[78] Kashpureff claims that at times "as much as three per cent of the Internet was running off our root name servers as opposed to the government's, which is very healthy, because that three per cent made a conscious choice to change."[79] By negotiating with additional Internet Service Providers, Kashpureff continuously tried to increase this number.[80] His efforts finally culminated in re-routing Internet users that were attempting to reach the "official" root name server to his own, alternative directory.[81]

The Kashpureff incident was neither the first nor the only one of its kind. On April 2, 1997, the Enhanced Domain Name System ("eDNS"), formed by several individuals hoping to provide a DNS alternative, went online.[82] It also implemented its own domain name structure. A sophisticated registration system ensured that no organization could control more than ten TLDs.[83] Similarly, there are alternative root servers such as New.Net[84] which has created more than 160 alternative extensions in six different languages,[85] including TLDs like .law, .school, .arts, and .church. According to ICANN itself, many people and entities[86] have set up alternative root name servers, apart from the examples mentioned here.

One may take two lessons from the foregoing discussion. First, the Internet is far from being an "intangible nowhere" that does not belong to anyone. Rather, the Internet can be perceived as a service provided by those

78. *Id.* at 5.

79. *Id.*

80. Friedman & Siebert, *supra* note 76, at 657.

81. Diamond, *supra* note 41, at 6 (stating that "[i]f you ask a DNS server to look up a name it doesn't know, it locates and queries a server that can provide the address, which sends the information to you. The query format includes an 'additional data' field with space for extra information. In this case Kashpureff used that field to his own ends, apparently sending off a message saying that www.internic.net referred to his IP address. Although Kashpureff provided a link to InterNIC, this trick sent traffic intended for InterNIC to his own AlterNIC Web site."). A discussion of Kashpureff's criminal liability is available. *See generally* Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users": Have you ever Heard of It?*, 6 RICH. J.L. & TECH. 23 (2000).

82. Levi et al., *supra* note 8, at 456.

83. *Id.*

84. *See, e.g.*, Catalogue of the English extensions, New.Net, *available at* http://www.new.net/index_ext.tp?lang_id=english (last visited Feb. 15, 2004).

85. The languages include English, Spanish, French, Portuguese, German, and Italian.

86. InterNIC, *supra* note 9.

who own and operate its infrastructure: the backbones and the root name servers. These entities make the Internet work for its users, just as those who operate the infrastructures of the telephone system provide a private service to telephone users. Whoever controls the root name servers controls the Internet.[87] If development and operation of the current Internet infrastructure takes place under the auspices of the United States, then the United States and its private organizations that are involved in the operation rightfully set the rules. As such, any argument that the Internet is a public domain in which every country must have its share is untrue.[88]

The second lesson one can take from the preceding discussion is that domain names are not unique. ICANN's assignment of a specific domain name to an individual user does not mean that the domain name is lost or is permanently purged from the pool of limited domain names available to the public. It simply means that the domain name is registered with the root name server controlled by ICANN. Every country and every individual is free to start another root name server and may assign the very same domain name to a different user.[89]

VI. Establishing a New Regime under National Sovereignty

Once the myth that cyberspace is unique and intangible is dispelled, then the traditional frameworks of the global telephone and postal systems may be evaluated as possible solutions to the dilemma of cyberspace governance. A system of decentralization in which every country retains its share of control may be a feasible way for the Internet to operate. It could be a way to solve fundamental problems of the DNS without abolishing domain names.[90]

A. The Cornerstones of a New Regime

As demonstrated by the examples of the telephone and postal systems, the new regime of Internet governance should encompass several cornerstones. First, every country, or a group of several countries, should run its own root name server. Ideally, each country would use the root name server already in operation for its national top-level domain. The country would be free to introduce new top-level domains[91] and to assign domain names to

87. *See generally* Diamond, *supra* note 41.

88. gTLD-MoU, *Draft of Memorandum of Understanding for the Internet Council of Registrars*, *available at* http://www.gtld-mou.org (July 17, 1997) (stating "[T]he Internet Top Level Domain (TLD) name space is a public resource and is subject to the public trust").

89. *See* Lemley & McGowan, *supra* note 10, at 611 (offering alternate ways to utilize domain names).

90. Liu, *supra* note 27, at 618 (stating that abolishing domain names is a radical solution to the domain name coordination problem).

91. Top-level domains are the equivalent to area codes in the telephone system.

individual users.[92] The country would have absolute legal and physical control over the assignment and routing of domain names, just as it does over the assignment and routing of telephone numbers and its national postal system.

Not merely acting as a national registrar as under the current DNS, each country would depend on an entity located inside its territory and would not be controlled by foreign legislation. The assignment of domain names could then be viewed as a sovereign right of the state, governed by national laws, very much like the assignment of telephone numbers and the creation of postal addresses. Such a system would rest upon a transparent and firm legal foundation, scarcity and traffic overflow would be reduced to a non-threatening level, and many trademark disputes would become obsolete. A nationalized system would allow limited concurrent use of the same trademark in different national geographic areas (according to the recognized principles of general trademark law).[93]

Specifically tailored national legislation would ensure the treatment of domain names in the proper context: *sui generis* rights that differ from pure trademarks, traditional business or individual names, and from telephone numbers.[94] Domain names combine some features of all of these traditional legal frameworks and can therefore not be governed effectively by the laws that regulate only trademarks, names, or telephone numbers. Specific national domain name legislation should address the application and registration process, dispute resolution mechanisms and questions of abandonment and cancellation. Furthermore, the legislation should provide guidance as to the adjudication of domain names in the case of competing claims.[95]

92. The equivalent to local phone numbers in the telephone system.

93. *See* Liu, *supra* note 27, at 606.

94. In the United States, some legislation specifically tailored to domain names exists already. *See, e.g.,* Anticybersquatting Consumer Protection Act, 15 U.S.C. §§ 1125(d), 1129 (2000) (prohibiting the bad-faith registration of someone else's trademark or personal name as a domain name); *see also* ICANN, *Uniform Domain Name Dispute Resolution Policy*, *available at* http://www.icann.org/udrp/udrp.htm (last visited Feb. 15, 2004) (outlining the policy under which accredited dispute resolution providers adjudicate cases of bad faith and abusive registration of domain names that violate trademark rights).

95. For instance, several individuals whose last name is "Smith" would like to register the domain name www.smith.com. It proves rather difficult to decide who should get the domain name and why, given that all claims are equally strong. The same issue arises with generic domain names: which one of all the travel agents in a country should be entitled to the domain name www.travel agent.com? These problems are novel, because trademark laws in most jurisdictions do not allow the registration of personal names. *See* 15 U.S.C. § 1052(e)(4) (2000). Nor does trademark allow the registration of generic terms. *See* Kellogg Co. v. Nat'l Biscuit Co., 305 U.S. 111, 112 (1938). Accordingly, trademark law does not provide answers to these questions. One approach to solving the problem has been the idea of "domain sharing." The idea is that there would be one "gateway" page under the common name pro-

With different autonomous national internets, the system would require an authority to ensure interoperability.[96] Internationally, a root server would be necessary to handle the traffic between different countries, just as is the case with the global telephone system.[97] Only if the national internets interconnect with a transnational parent network can the global character of today's Internet be maintained. This task should be performed by an international organization based on the International Telecommunications Union model. Unlike ICANN and NIS, it would neither be concerned with the introduction of new TLDs nor with the assignment of domain names. Its only task would be to set out the technical standards that ensure interoperability. Because this is a clearly defined task for the good of all member states, there would be fewer disputes as to which country should have how much influence on the decision making process.

As a technical matter, the coexistence of identical domain names in different countries throughout the world would require preceding "country codes" that make them distinguishable from one another, just like the country codes in the telephone system distinguish identical phone numbers in different countries from one another. Because, under the proposed system, a domain name like "www.travelagent.com" could be registered by different individuals in different countries, country codes would be necessary to direct the request to the desired website via the root name server in the specified country. In other words, a user could determine if he wanted to retrieve the website "www.travelagent.com" from the United States, Canada, Germany, Australia or any other country, simply by choosing to query the root name server of the desired country. The user would include the specific "country request" into the query sent to the nearest name server.[98] The general routing task would then be accomplished by the international root name server. A request without a specific country code would, just as a telephone call without a preceding country code, be directed to the website registered in the country from where the request originates.

Internet users from all countries would benefit greatly from such a system: by typing "www.healthinsurance.com" in a browser, a user would always find a health insurer in his or her own country rather than in some distant part of the world.[99] If the user were looking for a health insurer in a

viding access to all individuals or companies either bearing that name or conducting business under the generic name.

96. Lemley & McGowan, *supra* note 10, at 559 (arguing "[s]ome governmental body will have to police interconnections, as is done in the telephone industry").

97. InterNIC, *supra* note 9.

98. The nearest name server is usually run by the Internet access provider.

99. For the telephone system, this convenience is a matter of course: if a user dials "1-800-healthinsurance" in the United States, the reasonable expectation would be to reach a health insurer in the United States and not, for instance, in South

specific foreign country, however, he or she would only need to enter the country code when accessing the site.[100] The Internet would thus become better structured, while user confusion and wasted search time would be reduced.

B. The End of the Internet's Global Character?

If a policy such as the one advanced in this paper were to be implemented, some analysts might feel that the "global character" of the Internet might be in jeopardy. Under closer scrutiny, however, these apprehensions prove to be false concerns.

1. Country-Specific Domain Names

The lack of nationalization and localization of the Internet is generally considered to be one of the most important factors furthering its unparalleled success. Such a belief is not entirely accurate because the Internet is "nationalized" already: over 243 different ccTLDs[101] through which we can retrieve websites from 242 countries already exist.[102] If a user is looking for a travel agent in the United Kingdom, for instance, such an agent can be found by inputting "www.travelagent.uk" into the browser; if one in Australia is needed, then one should enter "www.travelagent.au" into the browser. Since the concept of "country codes" as proposed in this article already exists in the form of national TLDs, implementing the plan proposed here will not adversely affect the global nature of the Internet. With the proposed system, the only difference would be that the country codes would precede the second level domain names rather than follow them. The end of a domain name would be formed by a TLD that has been introduced by the country for its territory (*e.g.*, ".com," which would then serve as a TLD only within the national boundaries rather than a universal TLD).

2. Different Autonomous Networks

A salient feature of the Internet to most causal users is the idea that the Internet is one global entity. In spite of the fact that many users feel that the Internet is "one" global net, it really consists of "tens of thousands of networks."[103] Technically, the Internet has always been a network of networks.

Africa. If the user is looking for health insurance in South Africa, the user must dial South Africa's county code before the rest of the number.

100. That means that worldwide operating companies like McDonald's, for instance, would have to register their .com domain name in each country separately in order to be globally present on the Internet. This can easily be done by the subsidiaries in each country.

101. *See* Internet Assigned Number Authority, *supra* note 25.

102. The reason for the discrepancy between the number of abbreviations and number of countries is due to the fact that Great Britain has two TLDs: .gb and .uk.

103. GREWLICH, *supra* note 31, at 54.

The project of the Internet II[104] illustrates this perfectly. A switch to the system proposed in this paper would not change the global nature of the Internet.

3. The "Global" Domain Name

Finally, some might worry that the transition proposed might destroy the global uniqueness of domains on the Internet.[105] The notion that each domain name can be associated with one single definite website seems to be among the most fascinating aspects of the Internet. No matter where a user accesses the Internet, if he or she enters "microsoft.com," then the user will get the same "microsoft.com."

However, the notion of one global website for a certain term already belongs to the past. Today, the user has a choice of "www.microsoft" in combination with 243 different national and an increasing number of generic TLDs. This fact is compounded by the increase in domain name scarcity: website operators have already been compelled to become creative in choosing domain names. For instance, if "www.golf.com is already registered, website operates can register similar names such as "www.golf-online.com" or "www.golf-web.net." In short, a user in search of "golf" is already confronted with an overwhelmingly wide choice of possible domain names, rather than being able to refer to *the* website associated with the term. The proposed system would cause no qualitative changes to this situation.

C. The End of Non-Interference?

Naturally, the Internet community may view the proposed system of governmental domain name registration under national legislation as undesirable since "government regulation of Internet traffic in any form makes a lot of people nervous."[106] History is clear, however, that the Internet has always been significantly subject to governmental interference. Even if many like to think that cyberspace is a playground for a community that makes its own rules, immune from the officials of the "real world," where states "have no

104. *See supra* Part III.C.

105. *See* InterNIC, *supra* note 9 (arguing that that with the spread of alternative root name servers, "users would lose confidence in the utility of the Internet").

106. Lemley & McGowan, *supra* note 10, at 559; s*ee also* Steve Lohr, *The Internet as Commerce: Who Pays, Under What Rules?*, N.Y. TIMES, May 12, 1997, at D1 (calling it "inevitable" that "the Federal Government will become increasingly involved in the affairs of the Internet, even if that role is more as a referee than as a regulator"); ICANN, *Fact Sheet*, *available at* http://www.icann.org/general/fact-sheet.htm (last visited Feb. 15, 2004) (arguing that the "informal structure represented the spirit and culture of the research community in which the Internet was developed").

sovereignty where we gather,"[107] nothing could be further from the truth.[108] The Internet was "born and brought up" as a child of the United States government, which has retained an undeniable control over its fate up to the present day. Other countries are scrambling to obtain their share of control over the Internet.[109]

Moreover, national courts have adjudicated thousands of Internet issues worldwide.[110] Be it criminal prosecution as in the case of the German branch of Compuserve,[111] the "seizure" of domain names, or one of the numerous cases of copyright and trademark litigation, courts have been heavily interfering with cyberspace from its very beginning. The virtual world has always been as much subject to the law as the real world.[112] Finally, the experience

107. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, *available at* http://www.eff.org/Publications/John_Perry_Barlow/barlow_0296.declaration (last visited Feb. 15, 2004).

108. *See* Lemley & McGowan, *supra* note 10, at 553 ("Things are not quite as simple as this, however. TCP/IP does not do everything automatically and without supervision, any more than do the stock exchanges, often cited as the most efficient of "unregulated" markets. Rather, there are a wide variety of rule-making groups that enforce standards on the Internet.").

109. It is conceded that the proposed system would make it easier for countries to censor content on the Internet by preventing their citizens from accessing certain foreign websites. From a technical point of view, however, such access restrictions are already possible today. As for the general accessibility of the Internet, a nationalized system would not pose a specific threat to it: even under the current system, every country is already free to regulate general access by passing legislation that affects its national access providers. Theoretically, every country could require access providers to charge high fees for general Internet access. Likewise, every country could pass legislation that generally prohibits the existence of access providers and public access of the Internet. In this respect, the proposed system would not make it more or less difficult to control national Internet access.

110. For a survey of the cases decided in U.S. courts, for example, see John F. Delaney & M. Lorrane Ford, *The Law of the Internet: A Summary of U.S. Internet Case Law and Legal Developments*, 1244 PLI/CORP 103 (2000).

111. LG München, 14 NEUE JURISTISCHE WOCHENSCHRIFT 1051 (2000).

112. Due to the fact that it is easy for members of the Internet community to operate from outside the territory of a state that wishes to regulate them, many jurisdictional and enforcement problems that occur over the Internet have contributed to the image of the Internet as "The Wild, Wild Web." *See generally* Shipchandler, *supra* note 16. These problems would remain even under the proposed system, because "it is not possible to limit Internet communications to a particular geographic area or state." *See* Röben, *supra* note 31, at 435. This is the price to be paid for having a global network. However, if a country exclusively controls the registration of domain names under its own national root server, it can, as an ultima ratio, cancel the registration of a certain domain name if the website "behind" it contains illegal material. This possibility is, of

with vanity telephone numbers shows that a government-run registration system can work fairly well. The assignment of vanity numbers is becoming increasingly important as their commercial value is being recognized by telephone users worldwide, yet the administrative process does not face the criticism that the DNS encounters.

VII. CONCLUSION

The perceived "uniqueness" of domain names is a phantom obstacle in changing the current domain name system, which faces numerous difficulties. Since the alleged "uniqueness" does not exist, a national domain name registration system, in which every country runs its own root name server and controls the assignment of domain names to individual users within its national boundaries, is feasible. Thus, the successful models of traditional communication as embodied in the international telephone system and in the worldwide postal system can be adopted for cyberspace. Such a decentralized system would be able to solve many of the problems inherent in the current domain name system.

During the transition period from the "old" system to a "new" system, the rights of the current domain name owners ought to be respected. While the legal nature of a domain name is not quite clear, the current domain name holders should not be deprived of interest they have presently in their domain name. Anything else could arguably amount to a governmental taking. One possible solution for a smooth transition would be to allow current domain name holders to keep their domain name rights in the country in which the domain name is currently registered. The owner of "www.travelagent.com" in the United States, for example, would keep this domain name in the United States. In all other countries, "www.travelagent.com" would become available for national registration.

Such a change would, of course, require an unprecedented cooperation between the countries of the world. A beginning could be the creation of regional internets, for example, within the European Union. Other regions could follow, starting a development that could finally result in the nationalization of the Internet as proposed in this article. The United Nations is, and will continue to be, an important platform to coordinate the future development of the Internet. Unless its Member States use this platform more effectively, vehemently pushing the issue on the international agenda, the current system is unlikely to change. The change, however, would most probably be a change for the better.

---

course, limited to domain names registered in that country and would involve a concept of in rem jurisdiction over the domain name as a defendant as opposed to personal jurisdiction over the domain name holder. Such a concept is already codified in the United States. *See* 15 U.S.C. §1125(d)(2) (2000).