ICANN: BETWEEN THE PUBLIC AND THE PRIVATE
COMMENTS BEFORE CONGRESS

By Jonathan Zittrain †

In July 1999, the Subcommittee on Investigations and Oversight of the House Commerce Committee held a hearing entitled "Is ICANN Out of Control?" Mr. Zittrain testified at the hearing; what follows is a revised version of his testimony that addressed the hybrid character of the Internet itself—neither public nor private—and the challenges facing ICANN due to its hybrid structure.

TABLE OF CONTENTS

> The town, a suburb of Mobile, Alabama, known as Chickasaw, is owned by the Gulf Shipbuilding Corporation. Except for that, it has all the characteristics of any other American town. The property consists of residential buildings, streets, a system of sewers, a sewage disposal plant and a "business block" on which business places are situated. A deputy of the Mobile County Sheriff,

---

† Executive Director, Berkman Center for Internet & Society and Lecturer on Law, Harvard Law School. I thank Catherine Manley, Diane Cabell, and Benjamin Edelman for helping me prepare this work, and Molly Shaffer van Houweling for valuable insights.

> paid by the company, serves as the town's policeman. Merchants and service establishments have rented the stores and business places on the business block and the United States uses one of the places as a post office from which six carriers deliver mail to the people of Chickasaw and the adjacent area. The town and the surrounding neighborhood, which can not be distinguished from the Gulf property by anyone not familiar with the property lines, are thickly settled, and according to all indications the residents use the business block as their regular shopping center. To do so, they now, as they have for many years, make use of a company-owned paved street and sidewalk located alongside the store fronts in order to enter and leave the stores and the post office. Intersecting company-owned roads at each end of the business block lead into a four-lane public highway which runs parallel to the business block at a distance of thirty feet. … In short the town and its shopping district are accessible to and freely used by the public in general and there is nothing to distinguish them from any other town and shopping center except the fact that the title to the property belongs to a private corporation.[1]

The Internet lies somewhere between Chickasaw and Mobile. This simple fact—figurative though it may be—creates the lion's share of the debates over regulation of the Internet and fair apportionment of its bounties. To explain: We are entering an era in which "Internet governance" and "Internet regulation" are becoming synonymous with control of the Internet itself, of its paths and protocols, as opposed to control over behaviors that people and institutions engage in while using the Net.

Of course, control of the Internet has direct implications for control of its users; for example, creating a next-generation Internet whose users are more readily identifiable than their predecessors might make it much easier to regulate everything from online gambling to the distribution of pornography. The more the Net becomes a feature of daily life for the world's population, the more important it may be for governments (and their constituencies) to assert control over the Internet's workings—particularly those workings which bear on the "regulability" of online behavior.[2]

Further, those who can assert a role in creating or maintaining Internet infrastructure stand to profit in rough proportion to the popularity of the Net itself. Who owns or controls various components of the Internet are

---

1. Marsh v. Alabama, 326 U.S. 501, 502-03 (1946).

2. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

therefore no longer backwater issues without need of formal resolution—for reasons of both profit and governance.

The Domain Name System ("DNS")[3] is a suite of protocols. It is one that is less necessary to the actual operation of the Internet as we know it than TCP/IP, but it is, currently, quite important to Internet navigation. The domain name system resolves addresses such as <www.harvard.edu> or <www.cnn.com> into unique numeric addresses. In turn, these unique addresses point to a single location on the Internet. The current implementation of the domain name system anticipates a set of databases—housed on servers, accessible at all times over the Internet—that allocate control over certain names to particular entities.[4] Thus, somewhere an entry in a database associates <www.harvard.edu> (and the ability to specify its numeric destination) with Harvard University, and <www.cnn.com> with the Cable News Network. To control the DNS protocols—or even the servers called for by the current protocols—is to control identity on the Internet.

Such control is appealing to trademark interests who wish to ensure that a name associated with a company does in fact resolve to that company's point of presence on the Internet. For example, whether <www.hertz.com> points to Hertz Rent-a-Car or to a site for oscilloscopes depends on who controls and makes policy for the creation of entries in the <.com> database.[5]

Furthermore, control of entries in the <.com> database could facilitate control of Internet content: those who dislike (or deem illegal) particular websites may find control over those sites' domain name entries a significant weapon in attempts to remove the sites from the Internet.[6] For example, if the <.com> database did not contain a record for

---

3. For a technical explanation of the domain name system, see Jon Postel, Information Science Institute, *Domain Name System Structure and Delegation*, Request for Comments 1591 (visited Nov. 22, 1999) <http://info.internet.isi.edu/in-notes/rfc/files/rfc1591.txt>; *see also* Milton Mueller, *Technology and Institutional Innovation: Internet Domain Names* (May 28-29, 1999) (unpublished manuscript, available from the author at <mueller@syr.edu>).

4. *See* Thomas v. Network Solutions, Inc., 176 F.3d 500, 504 (D.C. Cir. 1999); *See also* Postel, *supra* note 3.

5. For a discussion of <.com>, *see* Postel, *supra* note 3.

6. *See* David Schepp, *Network NSI in Tussle Over Nasty Words in Domain Names*, NEWSBYTE NEWS (May 14, 1999), *available at* 1999 WL 512913; Joel Michael Schwarz, *The Internet Gambling Fallacy Craps Out*, 14 BERKELEY TECH. L.J. 1021, 1052-1058 (1999) (suggesting that removal of domain name records would be an effective way to prevent access to Internet gambling websites).

<www.hertz.com>, the address would cease to function—making the corresponding site much harder to find.[7]

Control over domain names was not particularly important in the era before the widespread commercialization and public adoption of the Internet. The domain name system was not developed by a corporation in the way Microsoft developed Windows or MCI developed MCI Mail, an early proprietary electronic mail system. Nor was it developed by a government. The domain name system evolved as the result of a collaborative scientific experiment.[8] Understanding this helps us to understand the unwieldy, sui generis organization known as the Internet Corporation for Assigned Names and Numbers ("ICANN").

In response to the concerns over control—and the absence of settled authority on who was entitled to exercise it—the United States Government solicited recommendations on the future of Internet governance.[9] The result was ICANN. Since its inception in the fall of 1998, ICANN has sought to assert control over the root of the domain name system in the name of the Internet community. It has done so for the stated purpose of fostering the consensus-building processes entailed in creating calculable rules of domain name management and evolution[10]—order out of initially irrelevant but then increasingly tense chaos.

I. THE PUBLIC AND THE PRIVATE

The Internet's ever-increasing number of "nodes," including websites that one might visit through a web browser, are linked by both physical and logical networks. The physical networks, whether wire or wireless,

---

7. Indeed, the Motion Picture Association of America has gone on record stating that it would like to see a mechanism by which websites with copyright-infringing content could have their domain names revoked. *See* Berkman Center for Internet & Society, *Scribe's Notes XI Emerging Privacy Issues* (Oct. 31, 1999) (visited Nov. 14, 1999) <http://cyber.law.harvard.edu/icann/la/archive/scribe-103199.html> (summarizing comments by Ted Shapiro, Deputy Legal Counsel, Motion Picture Association (Brussels) at ICANN and the Public Interest: Pressing Issues).

8. The Internet originated as a defense project under the guidance of the Defense Advanced Research Projects Agency (DARPA). This early network, called ARPANET, consisted of four nodes located at UCLA, Stanford, UCSB and the University of Utah. *See* Improvement of Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826 (1998) [hereinafter The Green Paper].

9. *See* Request for Comments on the Registration and Administration of Internet Domain Names, 62 Fed. Reg. 35,896 (1997).

10. *See* ICANN, *Status Report to the Department of Commerce* (June 15, 1999) <http://www.icann.org/general/statusreport-15june99.htm>.

quite literally ensure that electronic signals can be passed from one node to another.

The logical networks provide successive layers of abstraction so that one can sit at ease at a given node's terminal and dispatch information to (and request information from) elsewhere without knowing how the wiring works. For example, thanks to Internet protocol ("IP") addressing, one can stamp a packet of information with a unique number representing another terminal's address and place it into the Internet's general shuffle of packets with confidence that it will reach its destination without one having to specify the physical route. Thanks to the domain name system one can enter a unique name—like <www.cnn.com>—and end up at CNN's website without having to know its numeric IP address.

These physical and logical networks are the roads of the Net. They are the lattices that integrate the various parcels of private cyberland into a web that can be nimbly traversed. One need only know the name or number of the desired destination, and instants later one is exchanging packets with the site in question.

A. Marsh v. Alabama Revisited

We have plenty of experience with the intertwining of public and private that characterizes Mobile and so many other cities. Private property exists in grids, with networks of publicly-maintained and publicly-owned roads helping citizens travel from one destination to the next. Decisions about these public roads—how wide to make them, what to call them, their respective speed limits—are made by municipal authorities serving the public interest, who are accountable through the processes of the administrative and, ultimately, elective and constitutional states.

We have less experience with company towns like Chickasaw: private property linked by private networks. Ms. Marsh sought to treat it as she might any other town; she stood on the sidewalk outside the post office and distributed religious literature. She was arrested for trespassing after the Gulf Shipbuilding Company, which owned the sidewalk, objected to her presence. The Supreme Court sided with Ms. Marsh, and the state's enforcement of its criminal trespass law on behalf of the company was blocked: "Whether a corporation or a municipality owns or possesses the town[,] the public in either case has an identical interest in the functioning of the community in such manner that the channels of communication remain free."[11]

---

11. *See* Marsh v. Alabama, 326 U.S. 501, 507 (1946).

In other words, Ms. Marsh could hand out her pamphlets and there was little the Gulf Shipbuilding Company could do about it. An unbounded ability to exclude, however, is only one stick in a bundle of rights we normally call ownership. The roads of Chickasaw likely still "belonged" to the company in other ways: Would anyone have questioned the company's prerogative to name its roads as it pleased?

In towns like Chickasaw and Mobile, one can get around with physical cues as readily as logical ones. If the town is well known enough to the traveler, the traveler can simply walk to the library or a friend's house without much regard for street names. Hence the hypothesis that the *Marsh* court would not consider a challenge to the Gulf Shipbuilding Company's proprietary street naming schemes, even though the court upheld the "public" character of those streets.

On the Internet, however, one relies on mnemonics. To visit a website, one must grasp its exact name rather than the physical details of how to get there. A browser is like a taxi driver and the user its passenger in an unfamiliar and constantly-changing landscape. "Take me to <www.harvard.edu>!" is the imperative that makes the territory navigable to the user, rather than "turn left at the next website and then stop at the first university one sees."

In addition, <www.harvard.edu> is easier to remember than <www.2yhf927.edu>, and thus the most visited websites tend to be ones with memorable names. In the absence of physical cues, labels are everything. As a result, there is more public interest in the scheme by which domain names are assigned than there is in the titling of private streets.

The street names in Chickasaw were the Gulf Shipbuilding Company's to disburse; the street names in Mobile are the municipalities' to give out. Who gives out domain names in cyberspace? The answer, it turns out, has been quite complicated, and represents a hybrid of the public and the private.

B. Quasi-private and Quasi-public Domain Naming Schemes

There exist wholly private, proprietary naming schemes apart from the domain name system. For example, RealNames is a company that matches up words with locations on the Internet.[12] With a RealNames plug-in, a user can type in a word or phrase and have the RealNames company send the user to the destination indicated by the word—wholly independent of DNS. RealNames could respond to a request for "bicycles" by sending the

12. *See* RealNames Corp., *RealNames Homepage* (visited Nov. 24, 1999) <http://www.realnames.com>.

user to <www.bicycles.com>, to <www.superbikes.com>, or to <www.cnn.com> for that matter. Presumably RealNames's decisions will be market-driven, based on guessing what the consumer is looking for.

There also exist proposals for wholly public naming schemes as well. For example, the United States Postal Service has sought to administer the <.us> top level domain ("TLD"), linking physical street addresses to domain names.[13] Such a scheme would be quite similar to the streets of Mobile: one's domain name would be a function of one's address, which is in turn decided upon by municipal bodies.

For now, however, the only universal mnemonic drifting comfortably above a squabbling set of directories and naming schemes is the domain name system, and it was developed by private individuals using public money—who did not claim to "own" the system in the sense of proprietizing it. Instead, these individuals, almost all of them engineers, tried to come to decisions on the developing of the naming scheme through consensus, and to ministerialize as much of the system as possible so that conflicts could be settled by an automatic (if perhaps unsatisfying) rule, such as "first come, first served" for domain names.

II. EVOLUTION OF ICANN

A. Early Management of Domain Name Policy

This job of consensus-building for the domain name system was until recently performed by IANA, the Internet Assigned Numbers Authority.[14] IANA was not incorporated; it had no legal personality. At its core was one figure, Jon Postel, a researcher at the University of Southern California. Postel did pioneering work on domain names and personally managed key aspects of the domain name system, including the vaunted root. He personally stewarded the <.us> domain—the country code he had designated for the United States—until the day when the U.S. government sought to actively manage the domain itself.[15] To many, Jon was a Solomonesque figure who applied an engineering talent to the various issues that came up, thought hard, and simply did the right thing to keep the process running smoothly.

---

13. *See* The United Postal Service, Comments in Response to NTIA Request for Public Comments (RFC) on the Enhancement of the .us Domain Space, Sect. V (Oct. 2, 1998), *available at* <http://www.ntia.doc.gov/ntiahome/domainname/Campbell.htm>.

14. Although its functions are now largely subsumed within ICANN, a website still exists for IANA at <www.iana.org>.

15. That day has not yet arrived.

Jon did much of his work with the help of government grants.[16] In addition to taking the lead in developing the system of domain names as we know it, he led a process for documenting standards. These standards are available as documents entitled RFCs ("Requests for Comments," even though they are often final drafts). The RFCs include the specifications for how domain names work, along with manifold other aspects of Internetworking.[17] The standards are not formally enforced by any commission or governmental entity; thus they are in some sense voluntary. However, if a computer on the Internet deviates from these accepted protocols, it runs the danger of incompatibility and dysfunction. The RFC protocols have become the lingua franca of the Net, thanks to the sum of thousands of individual decisions by network administrators and software designers to hew to them. In this sense, they are quite binding.

No one owns the RFCs: no private company has a patent on the processes they describe, or an exclusive copyright on the documents themselves, and they are open to adoption by anyone without license.[18] In this sense they are public. Yet they are not developed by governments. In this sense they are private. They are written under the auspices of the Internet Engineering Task Force ("IETF"),[19] itself unincorporated, without legal personality, and for which there is no particular membership fee since there is nothing explicitly to join. The IETF comprises a group of self-selecting engineers, most of whom participate in their spare time. These engineers discuss the protocols on email lists with each other. Occasionally, they gather for a meeting where they try to develop consensus around what will work best—as expressed through a collective "hum" at a physical meeting or a rough poll via an email list.

Much of the design of the Internet was and is thus accomplished by a non-traditionally organized group of people who came from relatively similar backgrounds and had little patience for highly formalized structures. This informal system appears to work best—i.e., it comes to consensus—when the issues under discussion are of apparent and genuine interest only to the engineers who have gathered to discuss them. Political

16. Under a contract from DARPA. *See* The Green Paper, *supra* note 8.

17. See the RFC Directory maintained by the IETF Secretariat at <www.ietf.org/rfc.html>.

18. The RFCs included a "copyleft"-like license intended to copyright some IETF materials (by the Internet Society, since IETF does not legally exist) for the purpose of ensuring that the standards are not proprietized. *See* S. Bradner, Information Science Institute, The Internet Standards Process—Revision 3, Request for Comments 2026, (Oct. 1996), *available at* <http://www.ietf.org/rfc/rfc2026.txt>.

19. *See* IETF, *IETF Homepage* (visited Nov. 16, 1999) <http://www.ietf.org>.

ramifications of designing a network one way versus another are often ignored or disclaimed.[20]

B. From the Technical to the Political

In the IETF setting, there are rarely clear competing interests at stake outside the realm of engineering. But there are two examples of interests that have catapulted the domain name system out of the sleepy meetings of the IETF and into the public eye. These are exactly the kinds of issues, beyond the technical, that led most of the parties to the domain name debate to see a new, much more structured IANA come about, and that are echoed in the Commerce Department's White Paper as a reason for trying to go beyond the earlier status quo.

First, there is significant concern about trademark. As described above, domain names have become the primary way to reach something on the Internet. They are written on buses and coffee mugs, and the easier they are to remember, the more valuable they are when the audience in question is the public at large. Thus, there are fights over domain name ownership. The old system of "first come, first serve," (indeed, for awhile, "first come, first serve, with no fee per name") has thus come under fire. Major trademark holders, somewhat late to the Internet themselves, found their marks already registered when they attempted to take up shop online. For example, <hertz.com> was taken by a domain name speculator, and <mci.com> was taken by Sprint. A major company is not afraid of initiating a lawsuit to claim what it thinks it is entitled to.[21] However, many companies prefer a simpler, less-expensive way to get to the bottom of the issue, perhaps a form of dispute resolution whose results are more expeditious—and possibly more generous—than those provided by courts. Finally, those who think they deserve a domain name held by another may want to know who has registered the name. Without solid contact information about the defendant, it is not easy to start a lawsuit. Some cheer this fact, if only for privacy protection reasons, while others lament it. Decisions about domain name system architecture and the handling of domain name registrations can bear on whether famous mark holders and others can easily assert claims over names. These trademark issues present

---

20. Contrary to its usual self-imposed technical limits to discussion, the IETF is currently debating whether to build wiretapping standards analogous to those of CALEA (Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001 et seq.) into Internet Protocol packets. So far the prevailing opinion appears to be that doing so would amount to designing a security flaw into the system. See the Raven listserv located at <http://www.ietf.org/mailman/listinfo/raven>.

21. I don't mean to suggest that the law says that every trademark holder preemptively owns her own mark plus a <.com> or <.net> at the end of it.

a good example of the desire of powerful interests to propose changes to the management of the architecture of the Internet with legal, as opposed to technical, justifications.

A second example of pressures on the system that are beyond the technical is the entrepreneurial forces that want to provide domain name registration services. The ministerial act of registering domain names[22] is itself a lucrative business.[23] When a lot of money is directly at stake, it is very difficult to have IETF-like informality at the apex of the pyramid. The power of the root of the domain name system is the power to designate *who* can register the names under a given top level domain like <.com> or <.org>. It is also the power to designate *what* top level domains exist. The root of the system declares that there exists a <.com> domain and that a computer in the custody of a company called Network Solutions, Inc. ("NSI") will fill in registrations under it.[24] Since the computer hosting the authoritative root has no data on a <.biz> domain, for almost all of us there *is* no <.biz> domain.

Domain names were developed and managed with little more than a series of handshakes and a set of traditions for many years. This speaks to the spirit that built the Internet, kept it running, and ultimately attracted the rest of us to it. However, the Net is no longer just a convenient means of sharing research results or a large-scale experiment in applied computer science. It is an increasingly important foundation of commerce, social activity and information exchange.

---

22. Registration of domain names consists of associating a holder with a name, and inserting the holder's desired destination address into a table that helps converts these names to the ultimate IP numbers required to find a site on the Internet. *See* Lockheed Martin Corp. v. Network Solutions, Inc., No. 97-56734, 1999 WL 965618, at *2, (9th Cir. June 8, 1999).

23. Network Solutions, Inc., the major player in the domain name business, is currently valued by investors at over $5 billion. See detailed quote information at <http://www.cnetinvestor.com/quote-detail.asp?symbol=NSOL> (visited Nov. 29, 1999). *See also* Courtney Macavinta, *NSI Beats Analysts' Expectations* (Oct. 28, 1999) <http://news.cnet.com/news/0-1005-200-1422067.html>.

24. In 1999, the Department of Commerce granted NSI a four-year extension of a 1992 exclusive deal allowing them to administer registration of names under <.com>, <.net>, and <.org>. The rates NSI is to charge dropped from $35 per name per year to $9, and its registrations went from "retail" to "wholesale." *See* NSI, *Change Coming in Domain Name Registration* (visited Nov. 19, 1999) <http://www.networksolutions.com/internic/internic.html>. Under the 1999 ICANN agreement, many other companies will be permitted to share this responsibility. *See infra* note 35.

C. The Need for a New Governance

Driven by the changing nature of the Internet and before the more recent U.S. government involvement, Jon Postel moved to formalize his efforts by organizing the Internet Ad Hoc Committee ("IAHC").[25] After a series of meetings, the IAHC produced the Generic Top Level Domain Memorandum of Understanding ("gTLD-MoU"), a plan by which new names like <.biz> could come about, managed by a formal structure largely dominated by the technical community.[26] While the IAHC had some of the trappings of officialdom and the gTLD-MoU had the aura of a treaty,[27] the plan failed. Jon Postel ascribed its failure to a lack of support by business interests and governments. The failure was made explicit by NSI's refusal to add the new gTLDs called for in the gTLD-MoU to the root.[28] The National Science Foundation ("NSF")—the entity that generated research funding for Jon Postel and IANA and brokered the original cooperative agreement by which NSI registered names—called for a halt to any substantive changes to the root until a way out of the stalemate was found.[29]

Ultimately the Department of Commerce took over responsibility from the NSF for bringing about a compromise, and drafted the "Green Paper."[30] After a round of public comment it then issued the "White Paper," a "statement of policy" calling for the private management of domain names in the public interest by an entity to be created specifically for this purpose.[31]

---

25. *See* Mueller, *supra* note 3.

26. The gTLD-MoU proposed the creation of seven new TLDs. *See* Establishment of a Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System (visited Nov. 22, 1999) <http://www.gtld-mou.org/gTLD-MoU.html> [hereinafter gTLD-MoU]; Mueller *supra*, note 3; *see also* Heather Mewes, *Memorandum of Understanding on the Generic Top-Level Domain Space of the Internet Domain Name System*, 13 BERKELEY TECH L.J. 235 (1998).

27. The document itself was placed in the custody of the International Telecommunications Union as individuals and entities became "signatories."

28. The authoritative root file was in NSI's custody, though Postel (as IANA) claimed the right to make changes. *See* Mueller, *supra* note 3.

29. In a October 2, 1997 letter to NSI, NSF stated, "Network Solutions, Inc.—as administrator of the root zone—is not authorized to take direction from any entity other than the National Science Foundation with regard to the functions that Network Solutions, Inc. performs under the cooperative agreement." *See* Don Telage, *The New Commercial Internet: Where Do We Go From Here?* (visited Nov. 22, 1999) <http://netsol.com/policy/telage199803/tsld013.htm>.

30. *See* The Green Paper, *supra* note 8.

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

The White Paper called for a new organization (referred to in the document as "NewCo") to administer the DNS, as well as to decide future administrative policy.[32]

In October, 1998, the Department of Commerce entered into a series of memoranda of understanding with the newly-formed ICANN to manage domain names. The government began to transfer its residual authority in domain name matters to ICANN. Of course, even the government's own authority in these areas was, ultimately, as unclear as it was formally uncontested.

ICANN's shot at managing the top level of domain names—including the creation of policies that, through a cascade of contracts, can bind individual domain name registrants[33]—is now solidified through a network of agreements inked among NSI, ICANN, and the government.[34]

D. The Public/Private Challenge in a Political Environment

Given the money to be made registering names, control over the root is more than just a technical function. Those who want a piece of the domain name registration action[35]—among them are those with competing claims to slices of it—may only support ICANN if they think it will generate responsive policies. At the very least, people trying to build or maintain a business like to know where they stand and they like to have it in writing. They prefer to have what one would call "calculable rules" so that they

---

32. *See id*. at 31,749. NewCo was specifically asked to do the following:

> (1) Set policy for and direct allocation of IP number blocks to regional Internet number registries;
> (2) Oversee operation of the authoritative Internet root server system;
> (3) Oversee policy for determining the circumstances under which new TLDs are added to the root system; and
> (4) coordinate the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet.

Id.

33. Any would-be registrar must be accredited by ICANN and sign an agreement to be governed by ICANN's policies. Thus, ICANN can effectively bar participation by those who refuse to acknowledge its rules. *See* ICANN, *Registrar Accreditation Agreement* (visited Nov. 23, 1999) <http://www.icann.org/registrars/ra-agreement-10nov99.htm>.

34. *See* ICANN, *Approved Agreements among ICANN, the U.S. Department of Commerce, and Network Solutions, Inc.* (visited Nov. 22, 1999) <www.icann.org/nsi/nsi-agreements.htm>.

35. As of November 19, 1999, thirteen companies were accredited as registrars and currently operational, thirty-seven were accredited, but not yet operational, and thirty-seven were awaiting final accreditation. *See* ICANN, *List of Accredited and Accreditation-Qualified Registrars* (visited Nov. 19, 1999) <http://www.icann.org/registrars/accredited-list.html>.

can build a business on predictable forces as opposed to a "hum" that can be heard one way or another.[36] Thus the authority to modify the root file, or veto attempts to change it, is something that almost every stakeholder agreed needed more systematic handling.

More systematic handling, but not less sympathetic to any powerful interest. As a matter of pure political calculus, the Department of Commerce needed the concurrence of every powerful party with an interest in domain name policy in order to achieve a successful transfer of domain name policy-making authority to ICANN. These claims included legal assertions of possession of parts of the system (such as those advanced by Network Solutions to the <.com> registry operation and data, or the U.S. government's claim to the root), as well as simple claims of interest in substantive domain name policies. The latter have been advanced by parties as diverse as Net engineering groups like the IETF, other governments (particularly the European Union), and various trademark interests. Each of these groups must be satisfied that its interests are represented in order for ICANN's authority to be unchallenged. Thus the idea of ICANN went hand-in-hand with the idea of a "consensus" body. Since every powerful interest might think it could wield influence over it, this new body would be framed as inherently non-threatening.

The idea of ICANN was also one of closure: an end to paralyzing fights over domain policy between Network Solutions and engineers like Jon Postel. A mere trade association model does not capture the breadth of ICANN's responsibilities and intended structure, both because of the diversity of Internet stakeholders and because of the powerful, quasi-regulatory decisions that ICANN will make. ICANN is supposed to act in the public interest, not beholden to any one stakeholder. It is as if a private "International Communications Commission," comprised of all interested parties with a vested stake, were to attempt to allocate radio spectrum that had never been explicitly designated a public resource.

E. Toward Private Civil Procedure and Administrative Law

To foster ICANN's acceptability among interested parties, the U.S. government's solicitation of ICANN, as well as the resulting bylaws, demanded public organization-like features on the part of ICANN, while at the same time extolling the virtues of private management. These public-like features include basic principles such as openness, representation, and due process.

---

36. *See* 2 MAX WEBER, ECONOMY AND SOCIETY, 956 (1978).

1. Openness

The easy part of openness is "sunshine" practices like open board meetings. But there will still be tendencies to have private consultations with staff, and even informal meetings among board members. After all, there cannot be a microphone everywhere; it may not even be desirable to have a microphone everywhere all the time.

In any event, openness goes far beyond open board meetings. It is an ethos, a way of conducting business that strives in good faith to be inclusive, clear, and genuine. For better or worse, ICANN has been saddled with typical private corporate baggage. After all, in form it *is* a private corporation. To call ICANN's chief policymaking body a "board" already endangers the spirit of openness—and obscures the fact that ICANN is "governing" in some important sense. ICANN is a private company with a public trust; its policies are "voluntary" as much or as little as are the IETF's RFC standards, and its contracts are binding once finalized. It makes policies that are explicitly meant to go beyond the technical—a decision on whether or not to make the domain name architecture more beneficial to famous mark holders at the expense of other interests is still a political one.

Under strong pressure from the U.S. government, ICANN took the step of opening its board meetings to the public in the summer of 1999.[37] Nonetheless, this leaves aside entire swaths of other governmental "openness" laws, such as sunshine laws, which cover meetings of principals outside public forums, and freedom of information laws providing for the production of documents upon request. ICANN will have to decide whether and how to adapt the openness mandate to its hybrid character.

2. Representation

Representation is a second area of difficulty for ICANN. The White Paper calls for ICANN to be a broadly representative body, both geographically and with respect to the interests involved.[38] But how does one weigh the different interests? Consensus is defined in this environment in such terms as "there does not appear to be any one complaining all that much" or "most people seem to agree, except for a few outliers." Therefore consensus will be elusive at times. After all, contested issues may of-

---

37. *See* Esther Dyson, *Prepared Testimony for the U.S. House of Representatives, Subcommittee on Oversight and Investigation*, Interim Chair of the Board of Directors, (July 22, 1999) <www.icann.org/dyson-testimony-22july99.htm> (responding to House Subcommittee on Oversight and Investigation's questions regarding ICANN's formation, structure, and policies).

38. *See* The White Paper, *supra* note 31, at 31,748.

ten be a zero-sum game, and in such cases someone will "lose" on a given policy decision. When they do, the losers might say: "There is no consensus. I do not agree with this." And yet, ICANN cannot be paralyzed when consensus is missing. Maintaining the status quo is itself a decision that may upset some stakeholders and may be systematically detrimental to the evolution of the domain name space. The first goal must be to ensure that the openness and deliberative processes are in place. After they have been established, ICANN may then try to forge consensus and compromise wherever possible. It may also seek consensus around principles, and use that to justify specific implementation decisions among a set for which none has majority support. But when consensus is impossible, ICANN will have to make decisions. Weighing the different interests will be a difficult challenge.

A "procedural consensus" requirement—eschewing calculable votes in favor of generating documents that tend to show (or not show) "consensus"—may produce a paradox: there will be no objective means of ascertaining consensus. Thus added power is placed in the hands of whomever is to determine whether consensus exists. To the extent that ICANN's task is thought of as merely gauging consensus—rather than making substantive policy judgments through a representative board whose ultimate votes may` be deemed to be proxies for consensus—ICANN's behavior will be unpredictable and difficult to second-guess. Strikingly, NSI's October 1999 agreement with ICANN exempts NSI from adhering to ICANN policies in the absence of numeric manifestations of consensus[39]—consisting of a majority of ICANN board members and a super-majority of votes from relevant subsidiary "supporting organizations."[40] The agreement also requires a "documentation of consensus" through written reports describing how many stakeholders were contacted about a proposed policy, and whether each agreed.[41]

Consensus is not demonstrated simply by assent of self-identified stakeholder corporations and other organizations. ICANN's bylaws provide that half of its board must be selected through an "at-large" elector-

---

39. *See* ICANN, *ICANN-NSI Registry Agreement* (visited Nov. 22, 1999) <http://www.icann.org/nsi/nsi-registry-agreement-04nov99.htm>.

40. *See id.* The ICANN bylaws provide for three Supporting Organizations ("SOs") to "assist, review and develop recommendations on Internet policy and structure." *See* ICANN, *Bylaws*, art. 6 (amended and restated Oct. 29, 1999) <http://www.icann.org/general/bylaws.htm>. They are the Address Supporting Organization, the Domain Name Supporting Organization, and the Protocol Supporting Organization. Each may name three directors to the ICANN board. *See id.; see also* ICANN, *Supporting Organizations* (visited Nov. 22, 1999) <http://www.icann.org/support-orgs.htm>.

41. *See* ICANN-NSI Registry Agreement, *supra* note 39.

ate.[42] Apparently this electorate is open to anyone who wants to sign up. A fear is that the only people who will sign up are the people who have direct stakes in the process, and therefore the process might become a race to the ballot box to see who can get in the most votes. In some sense, that is a normal election. But in another sense, it is a recipe for capture if a number of the interests that ICANN should be looking out for—perhaps the greater interest of the public at large—are not joining ICANN by becoming members, or members in representative proportions.

Jim Fishkin of the University of Texas is fond of telling the story of what happened when a poll concerning who would be *Time's* "Man of the Century" was put to the world through an open Internet poll. Mustafa Kemal Ataturk—hero of the modern Turkish state—emerged as the leader in all categories, eclipsing Bob Dylan as the best entertainer of the century and Einstein as the best scientist. A last-ditch effort was apparently mounted by Greece to vault Winston Churchill over Ataturk as best statesman.[43]

Assuming the vote was not fraudulent—i.e. no one voted twice—was Ataturk deserving of the best "entertainer and artist" mantle, or had there been capture in the election? In the absence of a framework of campaign finance laws, electoral abuse laws (and commensurate penalties), the specter of one entity paying a grassroots lobbying group to create the "astroturf" of public sentiment around an issue or candidate through vote-buying cannot be discounted. This is a prospect that is particularly threatening with ICANN so long as ICANN's work is abstruse and technical even if it is political as well. Understandably, would-be voters may not hasten to register as members or exercise their votes for domain name management responsibilities, even if they may legitimately wish to be represented in the process either by an elected representative, or an appointee. Thus are the decision making activities of the FCC, the Supreme Court, and the Commerce Department legitimized—perhaps more than they would be under criteria of "democratic representation" were their leaders chosen by direct election.

It is likely that ICANN will have to move forward with some form of electorate if only for political acceptance. Accountability to an open membership is a way of tethering ICANN so as to lessen the need for direct government intervention.[44] Currently ICANN appears to be moving to-

---

42. *See* Bylaws, *supra* note 40, at art. 5, sect. 4.

43. *See* Chris Morris et al., *Is This the Man of the Century?: Forget Mandela, Einstein, Gandhi, and Mao, Here's Ataturk*, THE GUARDIAN, Oct. 30, 1997, at 1.

44. ICANN's most direct form of accountability right now is to the U.S. government, whose memorandum of understanding phases in responsibilities slowly, and makes

ward adoption of an Electoral College model in which an open membership votes for a council, that in turn votes for at-large board seats.[45] This may be the worst of both worlds—indirection that does not lead to any more representation or stability, and lessens the value of an individual vote in terms of direct influence over the organization. A possible outcome will be low public participation coupled with high registration rates among warm bodies motivated (or paid) by distinct interests.

A number of groups led by the Markle Foundation, and ranging from the Berkman Center to Common Cause to the Carter Center, have recently joined (or re-joined) the fray.[46] This participation will be judged on the basis of how well it helps ICANN fashion an electoral system from something other than simply reasoning from first principles.

3. Due Process

Due process is another area of ferment. The idea is to ensure that people have a formal opportunity to be heard and afforded the chance to protest in a meaningful way if they think their rights are being trampled. The process developing within ICANN is one that struggles to adopt internal structures for guaranteeing due process and deliberation. For instance, once a policy proposal is made, it may be referred to one of ICANN's supporting organizations. In the case of the Domain Name Supporting Organization ("DNSO"), the proposal goes to one or more "constituencies" or cross-constituency working groups.[47] The constituencies deliberate, form views, and make recommendations to the DNSO.[48] After allowing

---

those responsibilities provisional for the duration of the MoU. *See* gTLD-MoU, *supra* note 26; National Telecommunications and Information Administration, *Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers* (visited Aug. 28, 1999) <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>. Another source of accountability, or control, is the Internet technical community, which has been allotted several seats on the ICANN board through its "supporting organizations," and which in any event could be sufficiently roused to make the current popular, authoritative root file a pariah. *See* Bylaws, *supra* note 40, at Art. 5.

45. *See* ICANN, *Resolutions Approved by the Board* (visited Nov. 23, 1999) <http://www.icann.org/santiago/santiago-resolutions.htm#anchor21816>; ICANN, *At Large Membership and Elections* (visited Nov. 23, 1999) <http://www.icann.org/at-large/at-large.htm>.

46. *See* Markle Foundation, *Markle Foundation Commits More Than $1 Million To Improve Internet Governance, Including Initiatives to Make ICANN More Publicly Accountable* (visited Nov. 23, 1999) <http://www.markle.org/news/Release.199911021044.1219.html>.

47. *See* Bylaws, *supra* note 40, at art. 6, sec. 2.

48. *See id.*

other supporting organizations a similar chance for comment, the DNSO makes recommendations to the ICANN Board.[49] The ICANN Board votes and decides.[50] At that point an internal reconsideration process can be invoked by someone who feels that the decision is contrary to ICANN's structure and bylaws.[51] If the challenge gets past this "appeal" stage, there is a structure emerging—still not here, to be sure—for an independent board of review, which will look at the disputed issue and may require the Board to come explicitly to a new judgment on the subject.[52]

In litigation, there is a need to balance due process with a means to authorize closure. This balance attempts to prevent abuse by those who may make frivolous claims in an effort tie up a policy within a structure. ICANN faces a similar tradeoff, and it must choose a structure to reach an appropriate balance. The initial instinct (more process rather than less, and without an overall sense of unifying structure) has led to a proliferation of committees, advisory bodies, supporting organizations, working groups, ad hoc groups and other entities, each struggling to define and understand its role in relation to the others. A shakeout seems inevitable and healthy, presuming that what remains approximates an ability to participate with a clear momentum toward closure.

III. WHAT IF ICANN FAILS

As we judge ICANN, it makes sense to be aware of the likely alternatives. I see three possibilities if ICANN fails.[53]

A. Son of ICANN

First, one can imagine the creation of a "Son of ICANN" which would try to reconstitute a new organization that would improve upon that which ICANN has not done so well. I am skeptical about the success of a second attempt because it may be difficult to energize increasingly cynical parties to try again for a new ICANN. Also, I am uncertain it would be any better.

---

49. *See id.*

50. *See id*.

51. *See* ICANN, *Preliminary Report, Annual Meeting of the ICANN Board* (visited Nov. 23, 1999) <http://www.icann.org/minutes/prelim-report-4nov99.htm>; Bylaws, *supra* note 39, art. 3, sect. 4.

52. *See* ICANN, *Principles for Independent Review, Final Report of the Advisory Committee on Independent Review* (visited Nov. 30, 1999) <http://www.icann.org/santiago/triac-final-report.htm>.

53. ICANN's failure in the short term is much less likely now that agreements among ICANN, NSI, and the U.S. government are in place. *See supra* note 34 and accompanying text.

Further, if someone believes he or she is going to lose out as a result of the actions of ICANN or its possible replacement, a perfectly rational approach may be to attempt to undermine the whole organization rather than live under what the person considers adverse policies. Therefore, there may always be attempts to destabilize ICANN in order to re-start the process, to throw the dice again and see what might come out. This is not to say that any criticism of ICANN is the result of sour grapes; rather, that in a healthy environment there will *always* be criticism, and indeed some of it will call for ICANN's end.

B. An Inter-governmental Entity

A second possibility is that ICANN's functions would be assigned to an inter-governmental entity. It is hard to imagine the U.S. government alone trying to continue domain name system management responsibilities for the very reasons stated in the White Paper[54] as well as the fact that national governments are waking up to the value of country code domains ("ccTLDs") and beginning to assert a proprietary interest in their management.[55] An international treaty organization is one possible way that governments could reach an agreement on how the DNS should be run.[56] It is not clear to me that such an organization would make policies that are any more in touch with the Internet community than those proposed by a well-functioning ICANN. More importantly, as the historical context suggests, the power of the root derives from the fact that a critical mass of system administrators and "mirror" root zone server operators choose to follow it.[57] A drastic turnaround in the management of Internet top-level

54. The reasons given included a desire for more competition in domain name registration, the need for a "more robust" management structure, and the impropriety of the U.S. continuing to manage an increasingly commercial Internet. *See The White Paper*, *supra* note 31, at 31742.

55. *See* Press Communiqué of the Government Advisory Committee, August 24, 1999, Santiago, Chile (visited Nov. 28 1999) <http://www.noie.gov.au/docs/gacmtg3_communique.htm>.

56. Such an organization might be structured similarly to the International Telecommunications Union which studies technical, operating and tariff questions and adopts recommendations on them with a view to standardizing telecommunications on a worldwide basis and includes operation subdivisions not unlike the IETF. *See* ITU, *ITU Homepage* (visited Nov. 30, 1999) <http://www.itu.int/>.

57. The root server system is a set of thirteen file servers, which together contain authoritative databases listing all TLDs. Currently, NSI operates the "A" root server, which maintains the authoritative root database and replicates changes to the other root servers on a daily basis. Different organizations, including NSI, operate the other 12 root servers. The U.S. government plays a role in the operation of about half of the Internet's root servers. Universal name consistency on the Internet

functions—either through a sea change in favor of much more aggressive government involvement, or one that purports to literally privatize the whole system (imagine auctioning it off to the highest bidder)—could result in abandonment of the network by the technical or user community. RealNames might seem a more appealing alternative to addressing than it has to date. Engineers who run the domain name servers (that in turn subscribe to the root server for information about domain names) might simply point the servers elsewhere. The web of contracts currently buttressing the natural network effects (that auger only one predominant naming scheme) do not yet reach to every Internet service provider. Universities, companies like Prodigy or the Microsoft Network, and large corporations could cease listening to Jon Postel's "legacy root" for authoritative information about <.com>, <.net>, and <.org>.[58]

C. Free Market

Indeed, this hints at a third possibility following a demise of ICANN: the market is simply left to its own devices. In the absence of another ICANN or an "acceptable" government takeover, a battle would be fought by existing market players for control of the current root. Either through technical or legal maneuvering, some private party would end up running the root, and it would likely not be structured to foster due process, checks and balances, nor consensus building in the manner of the ideal ICANN. In other words, the winner would be truly "private," rather than "private, public trust." Network Solutions, Inc. would likely continue to operate the <.com>, <.net>, and <.org> top level registry.

The new "owner" of the existing root would then compete against the for-profit and non-profit entrepreneurs who are experimenting with alternative naming schemes. These schemes would also substitute their respective proprietary decision-making for "public trust" authority in allocating names to a particular entity or site.

Internet users and their respective Internet service providers would be able to specify where they would like to get their domain name information and they could choose any alternative root authority that the market might offer. Alternately, they could choose to adopt entirely separate di-

---

> cannot be guaranteed without a set of authoritative and consistent roots. Without such consistency messages could not be routed with any certainty to the intended addresses.

The Green Paper, *supra* note 8, at 8828.

58. Several organizations have proposed alternative root systems. *See, e.g.*, Open Root Server Convention, Inc., Open-RSC Homepage (visited Nov. 20, 1999) <http://www.open-rsc.org>.

rectory and naming architectures that work independently of the domain name system. The problem is that there is such enormous benefit in having a single repository that it is difficult to switch out of a system that nearly everyone—and everyone's software—has inherited. Because of this, the likely result is either a continued dominance of the legacy system (and the private party controlling it), or "tipping behavior" through which a new naming scheme would predominate, and a different private party would end up with control of a new root. Either way, Internet naming would be run by a private entity answerable (presumably) only to itself or its shareholders, insensitive to market forces to the extent that its dominance is locked in through global use. Enforcement of individual countries' antitrust laws or other ad hoc mechanisms would be the primary instruments of preventing abuse of this new de facto "essential facility."[59]

IV. CONCLUSION

ICANN has inherited an extraordinarily difficult situation, with high expectations all around, and with almost no discretionary room to move. The set of realistic options for substantive policy making and procedural structure is quite small. For better or worse, ICANN faces swift dispatch if it strays too far from the desires of any of the mainstream Internet technical community, the United States and other governments (including executive, legislative, and judicial branches, which in turn may not agree) and powerful corporate interests. Indeed, those representing the "little guy" and/or those wanting a maximally unregulated Net—one where political concerns have no place in technical management—are quick to worry about capture of ICANN by one or another of these powerful interests.

The key in this critical transition period is for those entities more powerful than ICANN—governments, large corporations, the technical community—to give ICANN enough rope to demonstrate either that it can operate to foster trust and respect among disparate interests (the kind of respect that has even the "losers" in a given policy question know they got a fair shake), or show a conclusive inability to rise to the challenge.

---

59. *See* Henry H. Perritt, Jr., *International Administrative Law for the Internet: Mechanisms of Accountability*, 51 ADMIN. L. REV. 871 (1999); Teague I. Donahey, *Terminal Railroad Revisited: Using the Essential Facilities Doctrine to Ensure Accessibility to Internet Software Standards*, 25 AIPLA Q.J. 277, 293-300 (1997) (identifying economies of scale, network externalities, and intellectual property rights as creating barriers to entry in software markets); Thomas v. Network Solutions, Inc., 176 F.3d 500, 504 (D.C. Cir. 1999).

* * * * *

ICANN is fashioned as a private, public interest municipal government. It is independent of the government functions of any single sovereign. This is in keeping with today's *zeitgeist* that government regulation of the Internet—whether of its users or the very networks that it comprises—is anathema to its nature and harmful to its explosive growth. ICANN's roads thus are not the roads of Mobile.

Yet ICANN is to be apart from proprietary interests or behavior consonant with mere profit-making. Unlike the Gulf Shipbuilding Company, ICANN is intended to internalize notions and practices representing due process, notice and opportunity to be heard, and a balancing of interests—all in the public trust—in its administration of the top level functions that in large part define the Internet's nature. Its roads thus are not the roads of Chickasaw.

Indeed, the Gulf Shipbuilding Company's management of Chickasaw was an operation incidental to its core task of building ships. Today, the difficulties of running a private community with attention to the public interest—more than simply the interests of the market—are only slowly being worked through in the context of gated communities.[60]

ICANN's middle path is improvisational. It demands of ICANN a self-sealed structure that attempts to keep its politics from overflowing into the realms of countries that usually govern such systems or of the engineers who realized that their technical work on these systems was increasingly interrupted by non-technical disputes. If ICANN succeeds, it might serve as a model for the type of forum through which other Net-wide political issues might be worked out. The recent debates within the IETF about whether to build wiretapping into the next generation Internet protocol standards are sorely testing the IETF's desire to limit its jurisdiction to the technical.[61] The creation of such entities as the "Realtime Blackhole List," through which a few people can effectively exercise discretion over one's sending and receipt of electronic mail on the Internet (they do so for the purposes of reducing unsolicited "spam"), highlights the beginnings of an

60. For a discussion of this debate, *see* David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165 (1999) (tracing the history of the private security industry and the challenges it creates for the judicial system); Steven Siegel, *The Constitution and Private Government: Toward the Recognition of Constitutional Rights in Private Residential Communities Fifty Years After Marsh v. Alabama*, 6 WM. & MARY BILL RTS. J. 461 (1998) (considering the application of the Supreme Court's state-action theory to residential community associations).

61. The IETF debate about wiretapping and privacy issues may be viewed by subscribing to the Raven listserv at <http://www.ietf.org/mailman/listinfo/raven>.

era of private undertakings that have regulatory outcomes without any particular due process, representation or openness components.[62]

ICANN's power could evaporate quickly, whether through adverse litigation outcomes that trump its decisions, legislation by sovereigns seeking to seize or control the intangibles ICANN tries to manage, or through an attrition of attention by which network operators or users could seek to substitute a new, separate domain name system or set of naming databases in place of the old. With this evaporation may go the notion that a medium as distinct at the Internet calls for a commensurately distinct mode of governance, one that aspires to the best of private and public rather than the worst.

62. *See* Lawrence Lessig, *The Spam Wars*, THE INDUSTRY STANDARD (Dec. 31, 1998) <http://www.thestandard.com/articles/display/0,1449,3006,00.html>; *MAPS Real-time Blackhole List* (visited Nov. 30, 1999) <http://maps.vix.com/rbl>.