OPEN TECHNOLOGY INSTITUTE

DAVID G. POST AND DANIELLE KEHL

Controlling Internet Infrastructure

The "IANA Transition" and Why It Matters for the Future of the Internet, Part I

OPEN TECHNOLOGY INSTITUTE | @OTI | @NEWAMERICA | APRIL 2015

ABOUT THE AUTHORS

David G. Post is a Senior Fellow at New America's Open Technology Institute. Until his retirement in Fall 2014, Post was the I. Herman Stern Professor of Law at the Temple University Law School, where he taught intellectual property law, copyright, and the law of cyberspace. He is the author of *In Search of Jefferson's Moose: Notes on the State of Cyberspace*, the (co)-author of *Cyberlaw:Problems of Policy and Jurisprudence in the Information Age*, and has published numerous scholarly articles on intellectual property law, the law of cyberspace, and complexity theory. Post also holds a Ph.D. in physical anthropology, has published widely in the area of animal behavior and evolutionary biology, practiced high technology transactions law at the Washington DC law firm of Wilmer, Cutler & Pickering, and clerked for Justice Ruth Bader Ginsburg at the Supreme Court and the DC Circuit Court of Appeals.

Danielle Kehl is a Senior Policy Analyst at New America's Open Technology Institute. She leads OTI's work on Internet governance and Internet freedom-related issues, and has also written on a wide range of technology topics including encryption policy, NSA surveillance, net neutrality, universal service, and U.S. export controls and sanctions. In 2014, she served as an advisor on Internet-related issues for the U.S. Delegation to the International Telecommunication Union's Plenipotentiary Conference in Busan, South Korea. Prior to joining New America, she worked at Access, an NGO that advocates for digital human rights. She holds a B.A. in history from Yale University and was a Fulbright Fellow in Rwanda.

This paper is the first in a series of papers on the IANA transition to be published by the Open Technology Institute in the spring of 2015. The first paper explains the nature of the challenges and the opportunities presented by the transition. Subsequent papers will address in greater detail the substance of specific transition proposals now under development, and provide recommendations concerning implementation of the key components of a successful transition process.

ACKNOWLEDGEMENTS

The authors would like to thank to Annemarie Bridy, William Drake, David Johnson, Kathy Kleiman, Tim Maurer, Milton Mueller, Paul Rosenzweig, and Andi Wilson for their comments on an earlier draft. The final paper does not necessarily reflect their views.

EXECUTIVE SUMMARY

On March 14, 2014, the United States government announced its intention to end its direct role in overseeing the Internet's Domain Name System (DNS). The IANA transition, as it is called, is a moment of critical importance in the history of the global network and the relationship between network governance and government control. It is an extraordinarily complex undertaking, both technically and legally, and there is a great deal at stake—but only a small handful of people understand the full scope of the problems involved and can participate intelligently in the public discussion about what entity or system should replace the U.S. government's role in DNS oversight. It is thus an unfortunate combination of circumstances for informed decision-making and public discussion. This paper seeks to fill at least a part of that gap.

At its core, the Internet's DNS is a truly remarkable engineering achievement, and its effective functioning has been critical to the spectacular growth of the Internet over the past two decades. In order for the system to work well and to achieve its goal of universal name consistency, the activities of literally millions of individual domain operators must somehow be coordinated. These coordination tasks are conventionally grouped under three separate headings: coordinating the allocation of IP Addresses (the *numbers* function), coordinating domain name allocation (the *naming* function), and coordinating *protocol development* for both the naming and numbering functions. Beginning in the mid-1980s, these tasks were performed by a number of individuals, entities, and institutions—some private, some public, some commercial, some voluntary—under a complicated series of grants and contracts procured and funded by various arms of the U.S. government.

By the mid-1990s, the system started to crack, as increasing public awareness of the value of the DNS (and the Internet in general) led to the emergence of serious questions about a range of DNS policy matters, including the apparent absence of competition in the domain name market, the practice of "cyber-squatting," and the lack of any formal management structure and accountability mechanisms for an increasingly valuable global resource. In response to these concerns, in 1998 the U.S. government called for the formation of a new, not-for-profit corporation to develop and administer policy for the Internet's name and address system. Shortly thereafter, the Internet Corporation for Assigned Names and Numbers (ICANN) was born: a California-based non-profit corporation that, with the U.S. government's blessing, took over control of DNS policy-making through a series of agreements, brokered by the Department of Commerce's National Telecommunications and Information Administration (NTIA), between the new corporation and the operators of the various components of the DNS.

The '98-'99 transition was a success; hardly anyone on the Internet noticed when it took place. Yet NTIA's recognition of the newly-formed corporation was premised on a number of very specific promises that ICANN had made about the way it would be organized, the tasks it would undertake, and the manner in which it would undertake them—including commitments about the structure and selection of the ICANN Board, the implementation of a "Consensus Policy Development Process," and assurances that ICANN's role would be limited to a specific, narrow set of issues. To maintain some degree of oversight, NTIA retained control over one vital subset of DNS-related tasks: the so-called "IANA

Functions." The IANA tasks include (1) maintenance of a series of "Internet protocol registries," (2) allocation of Internet numbering (IP Address) resources, and (3) maintenance of the authoritative Root Zone File on the "A" Root server and the processing of any modifications to that file. This arrangement gave NTIA substantial leverage over ICANN's post-transition actions and operations, because re-opening the IANA contract procurement was both a serious and a credible threat to ICANN's central role in DNS management. Although it is difficult to say exactly how this oversight was exercised, or exactly how it influenced ICANN's actions, there is little doubt that it served as an effective "backstop" to keep ICANN in line over the past two decades.

The current IANA transition is the logical culmination of the sequence initiated in the 1998-'99 transition, and it presents a significant opportunity for the United States and for the global community of Internet users. Over time, the justifications for a special role for the U.S. government in managing the evolution of the Internet and its governance systems have considerably weakened, as a consequence of both the Internet's vastly expanding global reach and of questions about the U.S. government's ability to claim any kind of neutral "stewardship" role for itself with respect to Internet affairs. Particularly in the wake of the 2013 Snowden disclosures, there is considerable evidence that if NTIA had not voluntarily decided to begin the transition, other Internet stakeholders—including important elements of the technical community, foreign governments, and ICANN itself—would have tried to force its hand.

The IANA transition also has important symbolic significance: it is a formal recognition by the United States that the Internet, which the United States government helped usher into existence 30 years ago, is now truly a *global* public trust. The Internet's core infrastructure, rather than being the special purview of any one country's exclusive jurisdiction, needs to evolve in ways that benefit all users, world-wide. And a strong, consensus-based, non-governmental, multi-stakeholder institution at the policy-making center of the DNS is likely to be the best way to ensure that the Internet infrastructure remains free from undue governmental influence. Moreover, getting the transition right has broad implications for the evolution of the Internet governance system. Its success—or failure—could have a significant impact on the shifting dynamics of the global debate more broadly, affecting both the United States' credibility and the weight of its support for the multistakeholder model.

Yet the risks the transition poses are also high. The DNS is, by design, essentially invisible to the vast majority of Internet users, but if it were to break down, or fragment into multiple competing systems, the impact on Internet use around the world would be substantial. Furthermore, in the wrong hands control over the DNS can be leveraged into control over a much broader universe of Internet activity and communication than that encompassed by the DNS alone. Freed from U.S. government oversight, what is to prevent ICANN from inserting itself into global law-enforcement or governance role far removed from its core commitment to insuring that the DNS runs smoothly and efficiently?

The stakes are high, for everyone who uses the Internet and everyone who is concerned with its future development as a global communications platform. Designing a transition plan that achieves the goal of relinquishing the U.S. government's oversight over the DNS while eliminating (or at least minimizing) the risks will be a difficult task, one that will require considerably more public attention and debate than it has received up to now. This paper, by explaining the nature of the challenges and the opportunities presented by the transition, lays some of the foundation for that debate, as well as for subsequent papers in this series, in which we will address in greater detail the substance of specific transition proposals now under development, along with our recommendations concerning implementation of what we believe to be the key components of a successful transition process.

TABLE OF CONTENTS

INTRODUCTION

"The Commerce Department's reservation of ultimate policy authority over the root is a ticking time bomb that must either be defused carefully or allowed to explode unexpectedly at some point in the future."

Milton Mueller, *Ruling the Root* (2002)

On March 14, 2014, the United States government announced its intention to end its direct role in overseeing the Internet's Domain Name System (DNS), possibly as early as September 30, 2015. It sets up a moment of critical—and quite possibly historic—importance in the history of the global network and the relationship between network governance and government control. This paper forms the first part of a multi-part series on this transitional event (known, for reasons discussed below, as the "IANA Transition").

The IANA Transition presents enormous opportunities, and poses enormous risks, for the future of the global Internet on which the world's people now increasingly depend. The way in which it proceeds will potentially affect all Internet users, possibly in significant ways. It is also a prodigiously complex undertaking, technically and legally. The conversation surrounding the transition contains (at least, to the uninitiated) a bewildering array of acronymically-identified steering committees, working groups, supporting organizations, coordination committees and sub-committees, and the like,[1] and much of the discussion uses a technical vocabulary that is difficult for those of us who are not network engineers to comprehend. For those who have not been paying much attention to DNS-related matters up to now and who are largely unfamiliar with the details of DNS management—a category that surely encompasses almost everyone who uses the Internet—it can be next-to-impossible to understand precisely what the IANA transition entails, how it will work, the ways in which it could impact the Internet's fundamental underlying infrastructure, or the consequences it might have for the future of Internet communications.

It is thus an unfortunate combination of circumstances for informed decision-making and informed public discussion: a great deal is at stake for virtually everyone on the planet, but only a very small handful of people understand the full scope of the problems involved and can participate intelligently in the public discussion.

This paper is designed to help fill that gap. Its purpose is to provide the background information regarding the transition's technical and legal complexities necessary to understand the choices it presents, and to understand

1. See *Enhancing ICANN Accountability: Process and Next Steps*, available at https://www.icann.org/resources/pages/process-next-steps-2014-08-14-en, which describes the formation of the IANA Stewardship Transition Coordination Group (ICG) and the ICANN Accountability & Governance Cross-Community Group (CWG) (which includes the Cross-Community Working Group – Accountability (CCWG), which itself comprises 14 Design Teams, see https://community.icann.org/display/gnsocwgdtstwrdshp/Design+Teams+List, four Work Areas, and three Work Parties, see https://community.icann.org/display/acctcrosscomm/CCWG+on+Enhancing+ICANN+Accountability) and the ICANN Accountability & Governance Coordination Group (representing 13 separate Communities, including the ALAC, the ASO, the ccNSO, the SSAC, the RSSAC....). This gives some of the flavor of the difficulties one encounters in trying to understand or participate in transition discussions. We will have more to say about the complexity of the institutions involved in these transition activities in a subsequent paper in this series in which we address "accountability mechanisms."

why they matter for the future course of Internet communication. We begin by describing some DNS fundamentals, and the origins and development of the relationship between the U.S. government and ICANN in Part I. Parts II and III describe the stakes involved in the IANA transition—the opportunities it presents and the risks it poses, and our reasons for supporting the transition if (but only if) critical accountability issues are resolved. Subsequent papers in this series will address, in detail, the substance of the various transition proposals now under development, along with our recommendations concerning what we believe to be the key components of a successful transition structure.

I. HOW WE GOT HERE

The Internet's Domain Name System (DNS), the U.S. Government, and ICANN

Note to the reader: The IANA Transition cannot be understood without an understanding of the function of the Internet's "Root," and the function of the Root cannot be understood without understanding how the DNS goes about its job. Readers familiar with these matters may wish to skip this discussion and proceed to the next section on "DNS Management."

The DNS[2]

The Internet's DNS is a truly remarkable engineering achievement, and its effective functioning has, without question, been critical to the spectacular growth of the Internet over the past two decades. Its value to global trade and commerce and communication is immense; by any measure, the commercial consequences alone of a serious breakdown in DNS functioning would surely run to hundreds of billions, if not trillions, of dollars.[3]

The DNS accomplishes its fundamental task—resolving names into numeric IP Addresses so that messages can be properly routed (see **Box 1** for more detail)—in a most unusual way. Instead of maintaining a single telephone-directory-like file containing names and their corresponding IP Addresses—like the *hosts.txt* file used in the original design—the information required to resolve names into IP Addresses is scattered in, literally, millions of places all across the network.

To begin with, names are organized into hierarchically nested *domains*. The domains at the top of the name hierarchy—the so-called top-level domains, or TLDs (*e.g.*, *.com*, *.edu*, *.biz*, *.uk*, *.jp*)—can each contain any number of 2nd-level domains (*example.com*, *xyz.com*, *google.com*, *davidpost.com*, *microsoft.com*, etc. in the *.com* domain, for example); each 2nd-level domain can contain any number of sub-domains at the 3rd level (*graphics.example.*

2. Excellent non-technical introductions to the DNS can be found at http://www.isoc.org/briefings/020/, http://www.internetsociety.org/internet-domain-name-system-explained-non-experts-daniel-karrenberg, and http://intgovforum.org/Substantive_1st_IGF/briefing19.pdf.
The material in this section on DNS operation and management has been compiled largely from the following resources: Leiner et al., *A Brief History of the Internet*, available at http://www.isoc.org/internet/history/brief.shtml; National Research Council Committee on the Internet in the Evolving Information Infrastructure, *The Internet's Coming of Age* (2001); P. Mockapetris, *RFC 1034, Domain Names-Concepts and Facilities*, available at http://www.ietf.org/rfc/rfc1034.txt (1987); Socolofsky and Kale, *RFC 1180: A TCP/IP Tutorial* (1991) available at http://www.rfc-editor.org/rfc/rfc1180.txt; David G. Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace*, chap. 10 ("Names") (2009); National Academy of Sciences, *Signposts in Cyberspace: The Domain Name System and Internet Navigation* (2005), available at https://www.cs.cornell.edu/people/egs/beehive/narc-dns.pdf (hereinafter "NAS, *Signposts in Cyberspace*"); Janet Abbate, *Inventing the Internet* (2000); A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route around the APA*, 50 Duke L.J. 17 (2000), available at http://personal.law.miami.edu/~froomkin/articles/icann-main.pdf (hereinafter "Froomkin, *Wrong Turn*"); Froomkin & Lemley, *ICANN and Antitrust*, available at http://papers.ssrn.com/paper.taf?abstract_id=291221; Jon Weinberg, *ICANN and the Problem of Legitimacy*, 50 Duke L.J. 187, 2000; Hoffmann, *Topological Ordering in Cyberspace*, available at http://www.wz-berlin.de/tau/ot/member/hofmann.en.htm#vortrage; Rony and Rony, *The Domain Name Handbook: High Stakes and Strategies in Cyberspace* (1998).

3. Crocker et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," available at https://cdt.org/files/pdfs/Security-Concerns-DNS-Filtering-PIPA.pdf:

> "The DNS is central to the operation, usability, and scalability of the Internet; almost every other protocol relies on DNS resolution to operate correctly. It is among a handful of protocols that that are the core upon which the Internet is built.
> "The DNS is a crucial element of Internet communication in part because it allows for 'universal naming' of Internet resources. Domain names have in almost all cases been universal, such that a given domain name means the same thing, and is uniformly accessible, no matter from which network or country it is looked up or from which type of device it is accessed. This universality is assumed by many Internet applications....
> "Universality of domain names has been one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet...."

Box 1. The Development of the DNS

Every system of networked computing must have a mechanism enabling one computer to locate another. The mechanism designed for the Internet from its earliest days involves assigning every Internet "host" computer a unique numeric Internet protocol (IP) address—a unique 32-bit number, usually printed in dotted decimal form (e.g., 91.121.44.02). The Internet's routing system was designed to permit a user, knowing only the IP address of the computer he wished to reach, to send a message to that destination; because no two computers had the same IP address, it was possible to pinpoint any computer on the Internet simply by knowing its IP address.

In addition to a numeric IP address, each host computer on the early Internet also was designated by a name: "BBN-SRC," or "Orpheus," or "Inter-NIC." A Network Information Center—managed by Dr. Jon Postel at the Information Sciences Institute (ISI) at the University of Southern California—maintained a simple database file ("*hosts.txt*") associating the names of each computer on the network with its corresponding IP address. It was a simple phone-book style directory, and a copy of the *hosts.txt* file was sent each day to all machines on the network. A user knowing the name (but not the IP Address) of another computer on the network could send a message to that computer by searching her copy of the hosts.txt database to find the IP address associated with the name, and then inserting that address into the message header and passing it along for routing over the Internet.

This system worked well enough in the early days of the network, while the Internet was still relatively small; but it did not scale well as the network grew. By the early 1980s, though the number of connected computers on what was then known as the ARPANET was still measured in the hundreds, many of those involved in the system's design recognized that a different, more sophisticated system to resolve names into numbers was needed. To meet that need, Postel and his colleagues at the ISI developed the DNS, in more-or-less its current form.

com, *blog.example.com*, *info.example.com* beneath the *example.com* 2nd-level domain); each 3rd-level domain can contain any number of 4th-level domains (*admin.graphics.example.com*, *blog.graphics.example.com*, etc.); and so on, up to 128 levels deep.

Each domain must maintain a database (a "zone file") containing the IP Addresses associated with all subdomains one level beneath it in the hierarchy; this database file must be installed on a machine (a "name server") accessible to all Internet users. So, for example, the operator of the *.com* domain must maintain a name server containing a zone file with the IP Addresses for all 2nd-level domains in the *.com* domain:

Table 1. Example of the Zone File, .com top-level domain

2nd Level Domain	IP Address
example.com	192.42.45.1
xyz.com	90.15.127.127
…	…

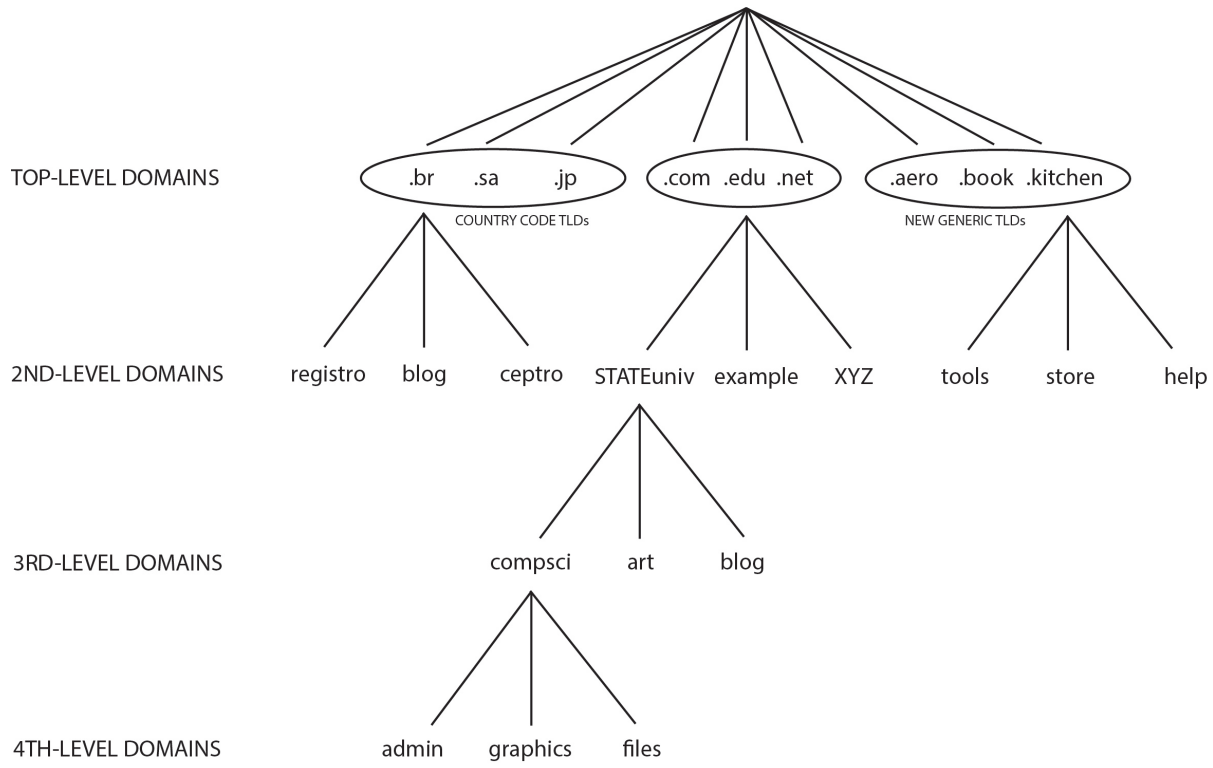
This structure repeats itself at each level of the hierarchy. That is, each 2nd-level domain must maintain a name server containing the zone file with the IP Addresses for all 3rd-level domains beneath it in the hierarchy. The *example.com* name server thus looks something like this:

Table 2. Example of the Zone File, *example.com* 2nd-level domain

3rd Level Domain	IP Address
files.example.com	192.42.96.96
graphics.example.com	192.42.127.1
archive.example.com	192.42.4.41
…	…

And so on for 3rd and 4th levels and beyond.

Given that a nearly infinite number of names can exist within this scheme, how does the DNS determine the IP Address corresponding to each of them, so that all messages can be properly addressed and routed to



How names are hierachically nested into domains, e.g. admin.compsci.STATEuniv.edu.

the intended recipient? How does the system ensure that an e-mail directed to someone at *admin.compsci.StateUniversity.edu*, or a request for the homepage stored at that URL, resolves itself correctly?

That process requires the sender (or the sender's Internet Service Provider) to take a number of steps:

1. querying the authoritative *.edu* name server to retrieve the IP Address for the 2nd level domain (*StateUniversity.edu*) name server;

2. using that IP Address, querying the StateUniversity name server to retrieve the IP Address for the 3rd-level domain (*compsci.StateUniversity.edu*) name server;

3. using that IP Address, querying the compsci name server to retrieve the IP Address of the 4th-level domain (*admin.compsci.StateUniversity.edu*).

Once that IP Address is received, it can then be inserted into the address field of the message and the message can be transmitted to an Internet router for delivery to that address.[4]

The Root

There is one important additional step omitted from the above account: How does the message sender obtain the IP address of the name server at the start of the process, *i.e.*, the *.edu* name server containing the authoritative *.edu* zone file?

4. Needless to say, although every Internet user performs this sequence of database queries countless times each day, the process is virtually invisible to the ordinary user. It all takes place in the background, mediated by software installed on user and ISP machines that manages the information retrieval and addressing process.

That information comes from one additional zone file at the very apex of the entire system, containing IP Addresses for the name servers associated with each of the top-level domains. The top-level domains, in other words, are not actually at the top level of the domain name hierarchy; there is an über-domain, as it were, above them. This domain is known as the "Root" domain, and its zone file—the one containing the IP Addresses of the name servers for all TLDs—is known as the "Root Zone File." That file is stored on a machine known as the "A" Root Server.[5] The Root Zone File is replicated ("mirrored") on 12 other computers (Root Servers B through M) scattered around the Internet. The "A" Root Server is the "authoritative" one in the sense that the other Root Servers rely on the "A" Root Server for any updates or changes to the Root Zone File, reproducing whatever version of the Root Zone File they receive periodically from it.[6]

DNS Management

The DNS' radically decentralized database design was one of the truly innovative elements of the early Internet. While it appears counter-intuitive and overly elaborate—a "magical mystery tour," as Tony Rutkowski, one of the early DNS pioneers, described it—requiring multiple queries for every message sent over the Internet, it has proven, over time, to be remarkably efficient, a critically important building block in the technical foundation that has allowed the Internet to scale to vast size as rapidly as it has.[7]

But decentralization like this comes with a cost; the day-to-day operation of the DNS is in the hands of literally millions of individual domain operators, from the Root Server operators all the way down to the operator of the *graphics.admin.compsci.StateUniversity.edu* domain (and the hundreds of millions of others similarly situated in the 2nd, 3rd, 4th, etc. levels). Their activities must somehow be coordinated if the DNS is to work well and achieve its goal of universal name consistency (*i.e.*, retrieving the singular IP Address associated with every named machine).[8]

Coordination tasks in the DNS are conventionally grouped under three separate headings: coordinating the allocation of IP Addresses (the *numbers* function), coordinating the allocation of domain names (the *naming* function), and coordinating development of the basic technical rules and standards for both the naming and numbering functions that ensure consistency across the entire system (the *protocol development* function). Beginning in the mid-1980s, these coordination tasks were performed under a complicated series of grants and contracts procured and funded by various arms of the U.S. government, including the Department of Defense, the National Science Foundation (NSF), and the Department of Commerce's National Telecommunications and Information Administration (NTIA). Responsibility under these early U.S. government grants and contracts for each set of tasks was divided up roughly as follows:

Numbers: Responsibility for coordinating the allocation of IP Addresses was assigned to the Internet Assigned Number Authority (IANA), a voluntary association of engineers headed by the aforementioned Jon Postel.

---

5. See https://www.iana.org/domains/root/servers. The "A" Root Server is located, at the moment, in Herndon, Virginia, at IP Address 198.41.0.4.

6. Between 1996 and 2001, the role of "authoritative" Root Server was actually transferred from the A Root Server to a "hidden primary" which is not itself accessible from the DNS, and all thirteen public root name servers (A through M) are now simply secondaries that mirror the hidden primary. VeriSign currently operates the hidden primary. For more information, see e.g. NAS, *Signposts in Cyberspace*, *supra* note 2, at 100.

7. See Weinberg, *ICANN and the Problem of Legitimacy*, *supra* note 2; *The Internet's Coming of Age*, *supra* note 2; Post, *Jefferson's Moose*, *supra* note 2, chap. 10.

8. For example, all Root Server operators must make the same Root Zone File, derived from the machine designated as the primary Root Server, available to Internet users; Internet users, and their ISPs, must choose a Root Server from among the same designated set of Root Servers at the start of the name resolution query; names and IP Addresses must be allocated in a manner that avoids duplicate registrations; the domain name/IP Address databases at all levels of the hierarchy must be formatted consistently, and must respond to queries, and process updates, in a consistent manner, etc.

IANA allocated blocks of numerical addresses to regional IP registries (RIRs)[9] who, in turn, allocated sub-blocks to Internet service providers (ISPs) in their respective regions; the ISPs, in turn, were responsible for IP Addresses to end-users.

Names: The day-to-day job of registering second-level domains in the top-level domains was handled originally by the Stanford Research Institute (SRI). In 1992, NSF entered into an agreement with Network Solutions, Inc. (NSI), a private company, to perform the registration services that had been handled earlier by SRI; NSI agreed to register second-level domains, on a first-come first-served basis, in four of the TLDs (*.com*, *.org*, *.net*, and *.edu*[10]) and to maintain those TLDs' zone files. NSI also had *operational* responsibility for the "A" root server; that is, the Root Zone File itself was under its control. But policy authority over the contents of the Root Zone File—in particular, the authority to decide whether a new TLD should be added to the "A" root zone, and who would be responsible for operating and administering each of the TLDs—rested with Jon Postel and IANA.

Protocols: The Internet Engineering Task Force (IETF), which had been performing protocol development regarding other Internet services (such as routing and message transmission), had responsibility for DNS protocol development. Responsibility for maintaining a "protocol registry"—the authoritative listing of all Internet technical parameters—was given to Postel and IANA.

The Consensus Unravels

By the mid-1990s, however, this allocation of DNS-related tasks, and these relationships, had become increasingly untenable—economically, politically, and even philosophically. The Internet had by then been transformed. What started as an obscure networking experiment used primarily by U.S. academic scientists and engineers had become, almost overnight, an indispensable tool of global commerce and communications. The transformation began in 1992, when commercial activity and commercial traffic were permitted, for the first time, on what was then called "NSF-NET."[11] It gained momentum with the release of the first World Wide Web browsers soon thereafter.[12] The "dot-com" boom had begun—the name nicely capturing the primacy, at the time, of the top-level domain in which everyone, suddenly, was very interested. Applications for new 2nd-level domains soared, especially in the *.com* TLD, which went from around 200 per month at the start of the NSF-NSI contract in January 1993 to over 30,000 per month by late 1995. By the time the NSF-NSI contract expired in January 1998, it had reached more than 200,000 applications per month—a 100,000% increase. As a result, the number of 2nd-level domains in the *.com* TLD went from under 15,000 in 1992 to over 1 million in January 1995 and over 8 million by 1998.

The technical challenges that this explosive growth presented were substantial, but the technical infrastructure of the Internet (including the DNS) absorbed the massive increase in network traffic without

---

9. There were originally three RIRs with the responsibility for allocating IP Addresses: ARIN for North America, RIPE for Europe, and APNIC in the Asia/Pacific region. Two additional RIRs have been added more recently, LACNIC (Latin America and the Caribbean) and AfriNic (Africa). See https://www.arin.net/knowledge/rirs.html.

10. The IETF's RFC 920 ("Domain Requirements") (October 1984), available at http://tools.ietf.org/html/rfc920, set out the first set of top-level domains: *.gov*, *.mil*, *.edu*, *.com*, *.org*, *.int*, and *.net* were the original "generic top-level domains." *See also* RFC 1591, available at http://www.isi.edu/in-notes/rfc1591.txt. The .gov TLD was restricted for use by U.S. government agencies and administered by the General Services Administration; similarly, .mil was reserved for use by and administered by the U.S. Department of Defense. The .int TLD was reserved for international treaty-based organizations like NATO and the United Nations. These generic TLDs were distinguished from the "country-code top-level domains," which would be identified by the "English two letter code identifying a country according the International Standards Organization (ISO) Standard for 'Codes for the Representation of Names of Countries'." See **Box 4** below for additional discussion of the distinction between the generic TLDs and the country-code TLDs.

11. See *Scientific and Advanced-Technology Act of 1992*, 42 U.S.C.§ 1862(g).

12. Just a few weeks after the NSI-NSF Cooperative Agreement became effective (December 1992) the first Internet browser – Mosaic – was released (January 1993), followed by Netscape Navigator in early 1994.

major adjustments.[13]

The policy infrastructure, on the other hand, proved more fragile. As the vast commercial potential—of the Internet as a whole, and of the DNS as a gateway through which individuals, institutions, and commercial entities had to pass in order to participate in Internet communications—began to be recognized and exploited, a spotlight was cast on the DNS and on the highly informal mechanisms under which it operated and was governed. Many serious concerns with the status quo, from many corners of the DNS ecosystem, were raised.

The US government was in the uncomfortable position of appearing to have created, and to be supporting and maintaining, a private monopoly—and a very lucrative one, at that—in the market for domain names. NSI's exclusive control over *.com* registrations, derived from its 1992 contract with the National Science Foundation, had become enormously valuable by 1994-95, and its growth curve and future revenue projections were astronomical.[14] Under the terms of the 1992 contract, the government had actually been paying NSI for each *.com*, *.org*, and *.edu* domain it registered. It was an arrangement that could be defended as a sensible use of taxpayer dollars in 1992, but not in 1995, by which time it had become clear that the system could and should be financed by users of the DNS services. The payments were discontinued in 1995, and NSI was allowed to charge users for registrations[15]; but that just exposed its monopoly position in the lucrative *.com* market to public view. It presented NTIA[16] with a series of monopoly pricing and rate-regulation questions—starting with: how much should NSI be allowed to charge for *.com* registrations?—of a kind the agency was largely unfamiliar with, and for which it was largely unprepared.

Trademark owners, and the trademark bar, were complaining more and more loudly to the Department of Commerce and Congress about what they regarded as an epidemic of "cyber-squatting" in the DNS. Cyber-squatting refers generally to the practice of registering a trademarked name (*e.g.*, Microsoft, Panavision, Hasbro) as a 2nd-level domain (most frequently in the *.com* domain, *e.g.*, *microsoft.com*, *panavision.com*, *hasbro.com*) by someone other than the trademark owner, for the sole purpose of selling the rights to the domain to the trademark owner.[17] Conflicts were becoming increasingly common and contentious, and mechanisms for the resolution of these disputes were either non-existent, or cumbersome and expensive.[18]

---

13. As the Internet continued to expand in the 2000s, one DNS scaling problem did arise: the use of 32-bit IP Addresses meant that there were "only" around 4 billion (2^32) IP Addresses available. At the time, it seemed like that would be sufficient far into the future; but by the mid 2000s it was clear that the limit was becoming a substantial constraint, and this has led to the development of IPv6, which uses 64-bit IP addresses.

14. On the strength of its control over domain name registrations in three of the TLDs, most notably *.com*, NSI raised over $50 million in an Initial Public Offering in September 1997, based on a valuation of over $20 billion, and the company was acquired by VeriSign, Inc. in 2000 for $21 billion.

15. See NSI-NSF Cooperative Agreement, Amendment 4 (Sept. 1995), at http://www.networksolutions.com/legal/internic/cooperative-agreement/amendment4.html, allowing NSI to charge $50 per year for domain name registrations.

16. Responsibility for managing these DNS contracts (including the Cooperative Agreement with NSI) was transferred from the research-oriented National Science Foundation to the Department of Commerce's National Telecommunications & Information Administration (NTIA) in 1998, see http://www.ntia.doc.gov/page/VeriSign-cooperative-agreement, reflecting the rapidly changing circumstances surrounding, and the rapidly changing political valence of, Internet-related policy questions.

17. "As there was no limit to the number of names a person could register, name speculators quickly understood that they could register names and attempt to seek buyers for them without risking any capital. While some speculators sought common words with multiple possible uses, a few others—who became known as cybersquatters—registered thousands of names that corresponded to the trademarks of companies that had not yet found the Internet and then sought to resell (or, some would say, ransom) the name to those companies. Since the Lanham Act requires commercial use before a court will find trademark infringement, it seemed more than arguable that mere registration, without use, was legal, and that the brokers/cybersquatters had found a costless way to profit." Froomkin, *Wrong Turn*, *supra* note 2, at 60.

18. See *id*. at 59-60 (describing NSI's "controversial" and "frequently amended" Dispute Policy regarding trademark-domain name conflicts). Trademark interests were also able to obtain an amendment to U.S. trademark law, the Anti-Cybersquatting Consumer Protection Act of 1998 (now codified at 15 U.S.C. §1125 (d)), to deal with cyber-squatting. *See generally* Jessica Litman, *The DNS Wars: Trademarks and the Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149 (2000).

Control of the Root was in play. Many members of the technical community involved in DNS management—notably including the still highly influential Jon Postel—began actively making plans in 1998 to open up the Root to large numbers of new TLDs. This was seen, in part, as a means of removing the entirely artificial scarcity[19] that was at the heart of the NSI monopoly and that had helped make names in the *.com* TLD so desirable and so valuable. That effort—informally dubbed the "Internet Ad Hoc Coalition" (IAHC)—took preliminary steps aimed at establishing a new registry for TLDs (a new, competing Root, in other words) to be managed by a Geneva-based "Council of Registries" set up under Swiss law.[20] At the same time, to many members of the trademark community, this opened up the unwelcome prospect of repeating the *.com* cyber-squatting debacle, and they insisted—quite vocally—that they would oppose any such expansion unless and until the cyber-squatting problem was dealt with.

Businesses seeking to invest substantial sums in building an online presence and to exploit the commercial potential of the new communications medium were dismayed by the apparent lack of any formal management structure, or accountability mechanisms, for managing the increasingly valuable DNS. Many of the major decision-makers—IANA, the IETF, the IAB[21]—had no formal legal status at all[22]; other important and increasingly contentious decisions appeared to be in the hands of a single individual (Jon Postel). To those seeking at least a degree of predictability for their investments, it looked like a rickety structure indeed. At the same time, the members of the technical community involved in DNS management—Postel included—were suddenly concerned about their exposure to liability for decisions that increasingly had very substantial financial implications.

---

19. Nobody seems to be entirely certain about the upper limit of TLDs that can be in the Root without causing DNS service disruptions or delays, see Froomkin, *Wrong Turn*, *supra* note 2 at n.12, but it is clear that the system can accommodate thousands of TLDs.

20. See Government Accountability Office, *Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers* (2000) (hereinafter "*GAO Report*"), at 6-7, available at http://www.gao.gov/new.items/og00033r.pdf; Froomkin, *Wrong Turn*, *supra* note 2, at 59-60; Mueller, *Ruling the Root*, *supra* note 2, at 152-55, for more detail on the IAHC initiative and efforts to unlink IANA from the U.S. government.

Efforts to wrest control of the Root away from the U.S. government (and away from NSI) came to something of a head on January 28, 1998, when Jon Postel sent an e-mail requesting that the Root Servers not controlled by NSI or the U.S. government start pointing to his server "B" rather than the "A" Root Server for the authoritative Root Zone File, a move that:

> "...would have enabled [Postel] to control the root and thus single-handedly create new TLDs. Most of the other root servers complied. To his detractors, Postel was attempting a power grab, a single-handed hijack of the Internet, or even threatening to split the root, creating the dreaded possibility of inconsistent databases.... When Ira Magaziner [who was by then the head of the White House Inter-Agency Task Force on DNS management] heard of what Postel would later diplomatically call a "test," Magaziner instructed Postel to return to the status quo. Postel did so, and the "test" was over. Magaziner was later quoted as saying that he told Postel that redirection could result in criminal charges, although it is unclear what statute would apply." Froomkin, *Wrong Turn*, *supra* note 2, at 64-5.

21. The IAB is the Internet Architecture [or Activities] Board; see *Internet [Architecture] [Activities] Board: Known History, World Internetworking Alliance* (1998), at http://www.wia.org/pub/iab-history.htm.

22. See *GAO Report*, *supra* note 20, at 35-6:

> "IANA was just one of several informal bodies that did much of the technical and policy decision-making for the Internet. Others included the Internet Engineering Task Force and the Internet Society. 'The legal authority of any of these bodies is unclear' as is 'the degree to which an existing body can lay claim to representing the Internet community...' the Federal Communications Commission observed in an early 1997 policy paper. That paper recognized the U.S. government's contribution to developing the Internet, but said the government 'has not, however, defined whether it retains authority over Internet management functions or whether these responsibilities have been delegated to the private sector.'"

The emergence of IANA was, as Milton Mueller describes it, something of a turning point in what he calls the "technical community's growing conception of itself as an autonomous, self-governing, social complex."

> "Explicit claims on the right to manage name and address assignment were being made by an authority structure that existed solely in Internet RFCs and lacked any basis in formal law or state action. The authority claims nevertheless had significant legitimacy within the technical community [because] Postel was known, respected, and trusted within the IETF and the supporting government agencies . . . One former NSF official described the situation as an 'enlightened monarchy in which the federal government funded the best brains. Their output was RFCs, which were approved through a collegial, though sometimes brutal, process of someone advancing an idea and everyone beating on it until the group consensus was that it would work. These RFCs became the 'law' of the internet – 'law' in the sense of operational practice, not legal jurisdiction." Milton Mueller, *Ruling the Root*, *supra* note 2, at 94-5.

The Internet's global expansion brought increasing complaints from abroad and increasing awareness at home concerning U.S. dominance of DNS affairs, and the global reach of Internet policy decisions.[23] All of this made the U.S. government's special management position increasingly anomalous (and politically charged[24]).

In 1998, in response to these concerns, the U.S. government announced, in an NTIA-issued Statement of Policy that became known as the "White Paper," that it was

> "…prepared to recognize, by entering into agreement with, and to seek international support for, a new, not-for-profit corporation ["NewCo"] formed by private sector Internet stakeholders to administer policy for the Internet name and address system [and] to undertake various responsibilities for the administration of the domain name system now performed by or on behalf of the U.S. Government or by third parties under arrangements or agreements with the U.S. Government."[25]

In the White Paper, NTIA set forth a number of conditions that would have to be met before the government would "recognize" any such entity. NewCo was to be "headquartered in the United States, and incorporated in the U.S. as a not-for-profit corporation," operating "for the benefit of the Internet community as a whole." It would undertake to "set policy for allocat[ing] IP number blocks to regional Internet number registries," "oversee operation of the authoritative Internet root server system," and "develop policy for determining the circumstances under which new TLDs are added to the root system." Governance of the new corporation was to be private (*i.e.*, non-governmental), operating under what NTIA referred to as the "multi-stakeholder model of Internet governance"; policies to be developed by the new entity that affected the "underlying functioning" of the DNS should be:

1. "arrived at [by] consensus," through a
2. "bottom-up process… reflect[ing] the bottom-up governance that has characterized development of the Internet to date," that is
3. open and transparent, so as to "protect against capture by a self-interested faction," and that
4. "includes all parties—businesses, technical experts, civil society, and governments—from the 'broad and growing community of Internet users,' ensuring "international participation in its decision making."[26]

NTIA furthered specified that NewCo would managed by a Board of Directors "balanced to equitably represent the interests of "IP number registries, domain name registries, domain name registrars, the technical community, Internet service providers (ISPs), and Internet users (commercial, not-for-profit, and individuals) from around the world." And, finally, the new entity was specifically tasked with solving the problems that had helped persuade NTIA to abandon its oversight role in the first place: to develop policies for (a) introducing competition into the domain name market,[27] (b) introducing new TLDs,[28] and (c) addressing the cyber-squatting problem.[29]

---

23. See Angela Proffitt, *Drop the Government, Keep the Law: New International Body for Domain Name Assignment Can Learn from United States Trademark Experience*, 19 LOY. L.A. ENT. L.J. 601, 608 (1999) (noting the concerns of the European Union, the Australian government, and others that the United States had "too much control over the DNS").

24. See *GAO Report*, *supra* note 20, at 19 (describing request for the *.ps* top-level domain by the Government Computing Center in the Occupied Palestinian Territory in 1996); Froomkin, *Wrong Turn*, *supra* note 2 at 47-48.

25. NTIA, "Statement of Policy, Management of Internet Names and Addresses," ("*DNS White Paper*"), 63 Fed. Reg. 31741 (1998), available at: http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses.

26. "[T]he Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management." *DNS White Paper* at #11.

"ICANN exists because the Department of Commerce called for it to exist."

Froomkin, *Wrong Turn in Cyberspace* (2000)

The Formation of ICANN

Shortly after publication of the White Paper, an entity that looked a great deal like "NewCo" materialized, in the form of a proposal submitted to NTIA bearing Jon Postel's imprimatur.[30] In November 1998, NTIA and this new corporation, now called the Internet Corporation for Assigned Names and Numbers (ICANN), entered into a Memorandum of Understanding (superseded by a "Joint Project Agreement" (JPA) in 2006), and a "Cooperative Research and Development Agreement" (CRADA) in 1999 (superseded by an "Affirmation of Commitments" in 2009).[31]

It is difficult to describe precisely the nature of the relationship between ICANN and the U.S. government, and it is difficult to find parallels elsewhere in U.S. administrative law and procedure. Although it was (and is) convenient to speak of NTIA "authorizing" ICANN to perform DNS management and DNS policy-making functions, or "transferring" the responsibility for those tasks to ICANN, that is not, technically speaking, accurate. As NTIA itself has pointed out on numerous occasions, it had (and has) "no legal or statutory authority to manage the DNS," and no regulatory power over DNS activities that it could transfer to ICANN.[32] ICANN does not act "for, or on behalf of" the U.S. government under its contracts with NTIA; those contracts refer instead to a "collaboration" on a "DNS Project" to "jointly design, develop, and test the

---

27. "Where possible, market mechanisms that support competition and consumer choice should drive the management of the Internet because they will lower costs, promote innovation, encourage diversity, and enhance user choice and satisfaction. [An earlier proposal to] move the system for registering second level domains and the management of generic top-level domains into a competitive environment by creating two market-driven businesses, registration of second level domain names and the management of gTLD registries.... [That] issue should be left for further consideration and final action by the new corporation. The U.S. Government is of the view, however, that competitive systems generally result in greater innovation, consumer choice, and satisfaction in the long run. Moreover, the pressure of competition is likely to be the most effective means of discouraging registries from acting monopolistically." *DNS White Paper* at #6(b).

28. "The challenge of deciding policy for the addition of new domains will be formidable. We agree with the many commenters who said that the new corporation would be the most appropriate body to make these decisions based on global input. Accordingly, as supported by the preponderance of comments, the U.S. Government will not implement new gTLDs at this time.... At least in the short run, a prudent concern for the stability of the system suggests that expansion of gTLDs proceed at a deliberate and controlled pace to allow for evaluation of the impact of the new gTLDs and well-reasoned evolution of the domain space." *DNS White Paper* at #7.

29. "The U.S. Government recommends that the new corporation adopt policies whereby domain name registrants would agree, at the time of registration or renewal, that in cases involving cyberpiracy or cybersquatting (as opposed to conflicts between legitimate competing rights holders), they would submit to and be bound by alternative dispute resolution systems identified by the new corporation for the purpose of resolving those conflicts. Registries and Registrars should be required to abide by decisions of the ADR system." *DNS White Paper* at "Revised Policy Statement: Trademark Issues."

30. This was, as Michael Froomkin put it, "no coincidence," as the "whole point of the White Paper had been to find a more formal structure for DNS management that left it in Postel's capable hands." Froomkin, *Wrong Turn*, *supra* note 2, at 70-71.

31. See http://www.ntia.doc.gov/page/docicann-agreements.

32. See the most recent NTIA "Report on the Transition of the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions," Jan. 31, 2015 (hereinafter "NTIA Report"), available at *http://www.ntia.doc.gov/report/2015/report-transition-stewardship-internet-assigned-numbers-authority-iana-functions*:

> "NTIA has fulfilled this temporary role [as the "as the historic steward of the DNS via the administration of the IANA functions contract"] not because of any statutory or legal responsibility, but as a temporary measure at the request of the President. Indeed, Congress never designated NTIA or any other specific agency responsibility for managing the Internet DNS. Thus, NTIA has no legal or statutory responsibility to manage the DNS."

See also NTIA's "Further Notice of Inquiry: The IANA Functions," 76 Fed. Reg. 34651 (2012), available at http://www.ntia.doc.gov/files/ntia/publications/fr_iana_furthernoi_06142011.pdf, explaining that while NTIA "does not have the legal authority to enter into a cooperative agreement with any organization, including ICANN, for the performance of the IANA functions" because it lacks "specific legislative authority" to do so, authorization for the contracts relating to the performance of the IANA Functions can be found in the "inherent authority [of federal agencies] to procure goods and services."

See also *GAO Report*, *supra* note 20, at 3-4:

> "Although the coordination of the domain name system has largely been done by or subject to agreements with agencies of the U.S. government, *there is no explicit legislation requiring that the government exercise oversight over the domain name system*.... The question of whether the Department has the authority to transfer control of the authoritative root server to ICANN is a difficult one to answer. Although control over the authoritative root server is not based on any statute or international agreement, the government has long been instrumental in supporting and developing the Internet and the domain name system. *The Department has no specific statutory obligations to manage the domain name system or to control the authoritative root server.*" (emphasis added)

mechanisms, methods, and procedures to carry out DNS management functions," and to undertake "a study for making the management of the root server system more robust and secure."

Rather than authorizing, or transferring authority to, ICANN, NTIA's role in the '98-'99 transition was a more subtle one of endorser and broker. NTIA's recognition of the newly-formed corporation as the appropriate steward for these DNS functions—bestowing on it the U.S. government's blessing, if you will—was critically important in securing ICANN's place in the DNS policymaking arena. In a system that runs largely on trust, and on the voluntary adherence by a large and geographically diverse population to specific standards and protocols,[33] that endorsement was reassuring and probably indispensable.

And just as important, NTIA managed to bring *all* of the parties with major policymaking and operational roles in the DNS ecosystem—Postel, IANA, the Regional Internet Registries, the IETF, and Network Solutions—into the deal, brokering a complicated set of contracts between and among these entities governing their respective roles in DNS operations and policy management. Precisely because ICANN did not (and could not) receive any "authority" to regulate the DNS from the Commerce Department, these contracts became the foundation for all of ICANN's policy-making authority.[34] "Contract-based governance of the Internet," Milton Mueller called it.[35] In broad outline, ICANN agreed to recognize (and implement, as necessary) the policy-making authority of IANA and the Regional Internet Registries for the "numbers" functions, and of the IETF for the "protocol development" functions.[36] Those entities, in turn—joined, most critically, by NSI, the incumbent registry operator for *.com* and several other TLDs[37]—agreed to accept ICANN's policy-making authority with respect to the remaining "naming" functions.

It was a considerable achievement, and it worked remarkably well. Hardly anyone noticed when the transition took place, and the DNS continued to function as smoothly on December 1, 1999, as it had the day before.

---

33. For example, as noted above, the complicated database-querying mechanics of the DNS name resolution process – the "magical mystery tour" described above – works as well as it does in substantial part because virtually all Internet users retrieve information from the same set of Root Servers; that occurs because their ISPs all use the same software program – BIND – to manage the querying process. See *ISC BIND*, Internet Software Consortium, at http://www.isc.org/products/BIND/.

34. See Froomkin, *Wrong Turn*, *supra* note 2, at 50 (explaining how the absence of any explicit NTIA or Commerce Department statutory authority for DNS management meant that "the critical legal documents are all contracts," and that, while ICANN's "contractual history *.is* complex, sometimes confusing, rich in acronyms, and at times perhaps a little boring, the legal underpinnings of the current DNS cannot be understood without a slog through it"). Chapter 4 ("The ICANN-based Contractual Web") of Bygrave's *Internet Governance by Contract* (Oxford Univ. Press: 2015) contains an outstanding analysis of the purely contractual basis of ICANN's powers.

35. Mueller, *Ruling the Root*, *supra* note 2, at 185.

36. See ICANN-IETF Memorandum of Understanding, available at http://tools.ietf.org/html/rfc2860, and the ICANN-ASO Memorandum of Understanding, https://aso.icann.org/documents/memorandums-of-understanding/memorandum-of-understanding/.

37. See Mueller, *Ruling the Root*, *supra* note 2, at 181-83 (describing how the NSI's "market power was the focal point" of the '98-'99 transition process, and explaining that any "refusal by [NSI] to participate in the new regime might result in the *de facto* privatization of the Root in its hands"); *GAO Report*, *supra* note 20, at 29-30:

> "In the fall of 1999, the Department signed agreements with ICANN and Network Solutions that included extending the Department's cooperative agreement with Network Solutions... Under these agreements, Network Solutions recognized ICANN and agreed to operate the registry for the *.com*, *.net*, and *.org* domains *in accordance with provisions of the Registry Agreement between ICANN and Network Solutions and the policies established by ICANN in accordance with the terms of that agreement*." (emphasis supplied)

See also Brendan Kuerbis, *The Last Third: Why the IANA Transition for Names is Hard*, available at http://www.internetgovernance.org/2015/02/10/the-last-third-why-the-iana-transition-for-names-is-hard/:

> "The communities that already had policy development organizations that predated ICANN's creation (IP addressing and Protocol parameters) never folded their operations into ICANN as envisaged. Indeed, the idea that policies related to Internet protocols would be developed in ICANN was dead on arrival. IETF opted almost completely out of the ICANN regime, and... the RIRs distanced themselves from ICANN, didn't sign an MoU with it until 2004, and made the Address Supporting Organization [within ICANN] into a vestigial entity used only for global policies. But for domain names, no pre-existing, independent policy making institutions existed. So domain name policy stayed inside ICANN."

ICANN and NTIA

One problem, however, remained. NTIA's recognition of ICANN was premised on a number of very specific representations and promises that ICANN had made about the way it would be organized, the tasks it would undertake, and the manner in which it would undertake them. For example, ICANN promised to (and did) insert into its By-Laws specific provisions declaring that it would:

- not "act as a Domain Name System Registry or Registrar or Internet Protocol Address Registry in competition with entities affected" by its policies;
- not "apply its standards, policies, procedures, or practices inequitably or single out any particular party for disparate treatment";
- operate "in an open and transparent manner," with a publicly accessible website, an annual audit, and various other review procedures;
- put in place a "reconsideration process" under which any person or entity materially affected" by any action taken by the corporation could "request review or reconsideration of that action by the Board of Directors";
- put in place an additional process for a more searching "independent third-party review of Board actions," which would be open to "any person materially affected by a decision or action by the Board," and which had the power to "declar[e] whether the Board has acted consistently with the provisions of those Articles of Incorporation and Bylaws";
- set up an office of Ombudsman, to act as "a neutral dispute resolution practitioner" providing "an independent internal evaluation of complaints by members of the ICANN community who believe that the ICANN staff, Board or an ICANN constituent body has treated them unfairly."[38]

There was a great deal more along these lines. ICANN committed itself to specific procedures for selecting Board members to insure both a degree of geographic diversity on the Board and a role for the each of the stakeholder groups in the selection process.[39] ICANN also agreed that it would implement a "Consensus Policy Development Process" through which DNS-wide policy would emerge.[40] That process was intended to produce "a consensus of Internet stakeholders," and it would be limited to a specific, narrow range of issues, namely issues for which "uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or Domain Name System ("DNS")."[41]

---

38. The original ICANN By-Laws, along with all subsequent versions, are available at https://www.icann.org/resources/pages/governance/bylaws-archive-en.

39. Although Board selection procedures were altered a number of times during ICANN's first few years, see Mueller, *Ruling the Root*, *supra* note 2, at 175-184, the basic procedure involves a number of directors (currently 8) chosen by a Nominating Committee, and a number (currently 2) from each of the three Supporting Organizations within ICANN (the Generic Names Supporting Organization, the Address Supporting Organization, and the Country Code Supporting Organization), and a number (currently 1) selected by the At-Large Community. The Nominating Committee, in turn, consists of representatives from various ICANN Advisory Committees (*e.g.*, Root Server System Advisory Committee, At-Large Advisory Committee) and Constituency Groups within the Generic Names Supporting Organization (*e.g.*, Business Users Constituency, Registry Constituency, Registrar Constituency, Intellectual Property Constituency, Non-commercial Users Constituency), and the IETF. See https://www.icann.org/resources/pages/governance/bylaws-en#VI. *See generally* Weber & Gunnarson, *A Constitutional Solution for Internet Governance*, 14 Col. J. Sci & Tech. 1, 11-14 (2012) (hereinafter "*Constitutional Solution*").

40. Appendix A of the original ICANN By-Laws, available at *https://www.icann.org/resources/pages/governance/bylaws-archive-en*, describes this policy development process in detail.

41. See ICANN-NSI Registry Agreement, Specification 1: "Consensus Policies shall relate to one or more of the following:

- issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or Domain Name System ("DNS");
- functional and performance specifications for the provision of Registry Services;
- Security and Stability of the registry database for the TLD;
- registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars;
- resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names); or
- restrictions on cross-ownership of registry operators and registrars or registrar resellers and regulations and restrictions with respect to registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or registrar reseller are affiliated."

These limitations on ICANN's policy-making authority are known, to ICANN insiders, as the "picket fence."

ICANN's representations and promises were a critical *quid pro quo* for NTIA's endorsement, and they were recognized as such by the parties to the original deal.[42] *But what was to keep ICANN from reneging on these promises once the transition had been successfully completed?* What assurances did NTIA—or, for that matter, the many millions of participants in the global DNS, from domain name registries in Korea to domain name registrars in Turkey to domain name registrants in Brazil, all of whom would henceforth have to comply with the policies set by the new corporation—have that ICANN would continue to comply with the representations and promises that it had made? What would keep it from altering its By-laws, say, to eliminate the prospect of "independent review"[43]? Or from modifying or even abandoning its adherence to policy-making by consensus of all stakeholders? Or from authorizing policies addressing conduct outside of the narrow limitations of the "picket fence"[44]? Given the absence of any legal remedy under the agreements with NTIA in the event that ICANN "misbehaved," (see **Box 2**) what would, or could, NTIA do then?

The IANA Functions and the IANA Functions Contract

NTIA's solution to this problem was to carve out and retain control over one vital subset of DNS-related tasks—the so-called "IANA Functions."

The IANA Functions comprise (1) maintenance of a series of "Internet protocol registries,"[45] (2) allocation of

---

42. See NTIA *Domain Name Agreements Fact Sheet* (Sept. 28, 1999), available at http://www.ntia.doc.gov/files/ntia/publications/agreements_factsheet_19990928.pdf:

> "ICANN will be contractually obligated, to the registry and to all accredited registrars, to comply with specified procedural requirements governing the exercise of its authority. These include (a) definition of the consensus required for action by ICANN and specification of the procedure for reviewing ICANN's determination that a consensus exists; (b) a commitment to open, transparent, and pro-competitive processes; and (c) a prohibition against arbitrary, unjustifiable, or inequitable actions ."

See also Weber & Gunnerson, *Constitutional Solution*, *supra* note 39, at 64:

> "Eschewing the very notion of 'a monolithic structure for Internet governance,' U.S. policy as expressed in the DNS White Paper sought only to inaugurate "a stable process to address the *narrow issues of management and administration of Internet names and numbers* on an ongoing basis." Later descriptions of ICANN's mission by the U.S. have been equally constrained. The U.S. Principles on the Internet Domain Name and Addressing System *described ICANN as "the technical manager of the DNS and related technical operations"* and stated that "[t]he United States will continue to provide oversight so that ICANN maintains its focus and *meets its core technical mission*." The JPA characterized ICANN's work as "the coordinator for the technical functions related to the management of the Internet DNS." Likewise, the Affirmation described ICANN as having the "limited, but important technical mission of coordinating the DNS." Statements like these demonstrate that the U.S. government—the body whose policy decisions led to ICANN's creation and whose contract with ICANN continues to give it authority over the IANA functions today—has consistently viewed ICANN's mission as "technical" and "limited." *The narrow mission for which ICANN was created marks the outer boundary of its legitimate authority. It was never intended to have an undefined reserve of powers over Internet governance...*" (emphasis added)

43. For example, after receiving an adverse Independent Review Panel ("IRP") decision in 2008 regarding its handling of the application for a new *.xxx* TLD, ICANN initiated a process leading to a change in the provision in its By-Laws dealing with independent review. The original provision, which charged the IRP with "comparing contested actions of the Board to the Articles of Incorporation and Bylaws, and with declaring whether the Board has acted consistently with the provisions of those Articles of Incorporation and Bylaws." The substitute provision, adopted in 2012, has a much *more* limited scope; the IRP would henceforth only consider whether the Board "act[ed] without conflict of interest... exercised due diligence and care, [and] exercise[d] independent judgment" in making any particular decision. See *Independent Review Bylaws Revisions*, available at https://www.icann.org/en/system/files/files/proposed-bylaw-revision-irp-26oct12-en.pdf.

See Weber & Gunnarson, *Constitutional Limitations*, *supra* note 39, at 69 (the current IRP process is a "paradigm of procedural unfairness" and the fact that "ICANN has no effective appeal mechanism is troubling, given ICANN's origins and its repeated written agreements with the United States"); Maher, *Accountability and Redress*, available at *http://www.circleid.com/posts/20140829_accountability_and_redress/* (describing ICANN's "manipulation of its By-Laws" as imposing a "severe limitation" on the IRP's powers, and suggesting that ICANN "decided that a change in the ground rules was needed in order to avoid further and similar embarrassments" after the *.xxx* debacle).

44. The "picket fence" refers to the set of limitations on ICANN's authority embedded in various contractual documents, see *supra*, note 41. See also Weber & Gunnarson, *Constitutional Limitations*, *supra* note 39, at 64 ("No one can seriously question that ICANN currently intrudes into areas beyond its technical mandate").

Box 2. The NTIA-ICANN Contracts

None of the contracts between NTIA and ICANN—the Memorandum of Understanding (1998), the Cooperative Research and Development Agreement (1999), the Joint Project Agreement (2006), and the Affirmation of Commitments (2009)—gave NTIA any real remedy in the event that ICANN breached its various representations and promises.

NTIA had the right to terminate those contracts if it were unhappy with ICANN's performance, declaring the "DNS Project" to have been a failure, withdrawing its endorsement/recognition of ICANN, and seeking some other partner to take on these tasks.

But what would happen then to the DNS? NTIA had no right to order ICANN to cease its DNS management activities after termination, no legal mechanism by which it could take these functions away from ICANN and transfer them to another party. As a consequence, any attempt to "un-endorse" ICANN and to substitute another entity in its place would almost certainly have produced a deep fracture in the DNS, with multiple, competing sources of supposedly "authoritative" name server information, and an end to universal name resolution and the unitary, Internet-wide DNS.

It was a kind of "nuclear option," destroying the system it was ostensibly trying to save. And like most nuclear options, it was largely ineffective as a mechanism to ensure contractual compliance, since all parties realized that it would only be exercised in the direst of circumstances.

Internet numbering (IP Address) resources,[46] and, most importantly, (3) maintenance of the authoritative Root Zone File on the Primary ("A") Root Server, and processing any and all additions, deletions, or other modifications to that file. Unlike the other DNS policy-formation tasks that ICANN would be undertaking—*e.g.*, regulating the competition between registries and registrars, instituting a process to resolve cyber-squatting disputes—the IANA functions *would* continue to be the subject of U.S. government procurement, performed on behalf of, and under the ultimate authority and direction of, the U.S. government.

The tasks required to maintain the Root were split into two parts—policy-making functions and operational functions—with two separate procurements and two separate contracts. NTIA awarded the operational contract for the Primary ("A") Root Server to Network Solutions, Inc. ["NSI," now VeriSign]. NSI/VeriSign would have physical control over the Root Zone File, and would operate and maintain the "A" Root Server where that file would be stored. It would be responsible for making any changes to the Root Zone File, but it would do so "at the direction of" NTIA, processing only those changes for which it received written authorization from NTIA.[47]

---

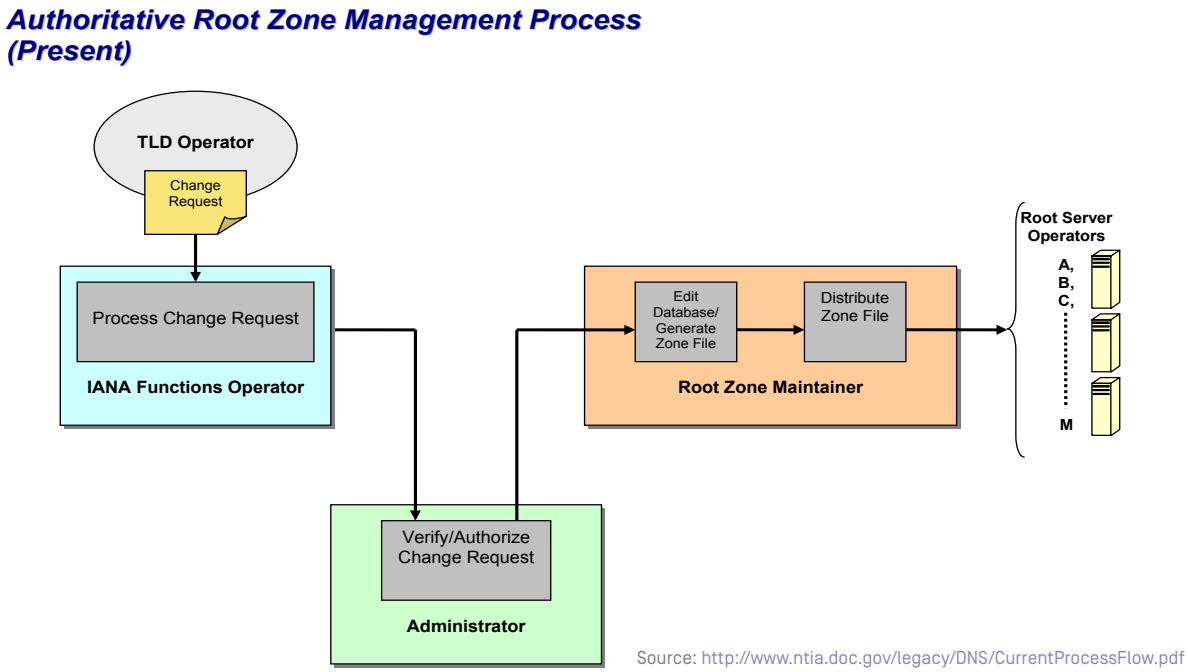
45. The IETF describes the function of the protocol registries this way:

> "Many IETF protocols make use of commonly defined protocol parameters. These parameters are used by implementers, who are the primary users of the IETF standards and other documents. To ensure consistent interpretation of these parameter values by independent implementations, and to promote universal interoperability, these IETF protocol specifications define and require globally available registries containing the parameter values and a pointer to any associated documentation. The IETF uses the IANA protocol parameters registries to store this information in a public location." See http://tools.ietf.org/html/draft-ietf-ianaplan-icg-response-09.

46. The IANA IP Address tasks refer to "the allocation of blocks of Internet Number Resources… to the Regional Internet Registries (RIRs) [and] the registration of such allocations in the corresponding IANA Number Registries." See https://www.nro.net/wp-content/uploads/ICG-RFP-Number-Resource-Proposal.pdf.

47. See *GAO Report*, *supra* note 20, at 27-28 (NSI/VeriSign operates "A" Root Server "at the direction of the Department [of Commerce]"); *NTIA's Role in Root Zone Management*, available at http://www.ntia.doc.gov/other-publication/2014/ntia-s-role-root-zone-management; NTIA *Fact Sheet*, *supra* note 42 ("NSI will continue to manage the authoritative root server in accordance with the direction of the Department of Commerce"). The NTIA-VeriSign agreement regarding maintenance of the "A" Root Server provides that:

> "While Network Solutions continues to operate the primary root server, it shall request written direction from an authorized [Department] official before making or rejecting any modifications, additions or deletions to the root zone file." See http://www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm.



Source: http://www.ntia.doc.gov/legacy/DNS/CurrentProcessFlow.pdf

How modifications ("change requests") in the Root Zone File are currently processed under the IANA Functions Contract, showing the relationships between ICANN (the "IANA Functions Operator"), NTIA (the "Administrator"), and VeriSign (the "Root Zone Maintainer").

On the policy-making side, NTIA awarded a second contract—the IANA Functions Contract—to ICANN. Under this contract, ICANN had responsibility for developing rules and procedures and policies under which any such changes to the Root Zone File were to be proposed, including the policies for adding new TLDs to the system. Here again, NTIA retained "final authorization authority"[48]; all such changes had to be transmitted first to NTIA for approval before they could be sent along to NSI/VeriSign for actual implementation in the Root Zone File.

This arrangement gave NTIA substantial leverage over ICANN's post-transition actions and operations. Because these "IANA functions," unlike the other DNS policy and management functions that ICANN agreed to perform, *were* being performed for, and on behalf of, the United States, NTIA could (and did) extract specific, contractually-enforceable promises from ICANN concerning its governance and decision-making structure and operations, and it included those in ICANN's "Statement of Work" under the contract.[49] More

48. See ICANN Security and Stability Advisory Committee, *Report on the IANA Functions Contract* (Oct. 20, 2014), available at https://www.icann.org/en/system/files/files/sac-068-en.pdf:

> "As the Root Zone Management Process Administrator, NTIA's role can be described as the 'Final Authorization Authority' for changes to the Root Zone content and contact information for the Top Level Delegations. This is the most significant technical and policy activity currently performed by NTIA that is related to IANA activities."

The Operator Technical Proposal for the IANA Functions Contract, available at https://www.icann.org/en/system/files/files/contract-i-1-31may12-en.pdf, provides that any proposed changes to the Root Zone File must be "transmitted to the Administrator [NTIA] for authorization [and] such changes cannot be enacted without explicit positive authorization from the Administrator."

49. The Statement of Work for the IANA Functions Contract (available at http://www.ntia.doc.gov/files/ntia/publications/icann_volume_i_elecsub_part_1_of_3.pdf) provides, for example, that ICANN will assign and register Internet protocol parameters "only as directed by" the IETF's Request for Comments process, that ICANN will develop "pertinent policy as it relates to [its] mission through a bottom-up, consensus-driven process with interested and affected parties," that policy Working Groups will be "open to everyone in ICANN's volunteer community" and that "all Working Group discussions will be recorded and transcribed [and] translated into the five non-English United Nations languages," and that ICANN will employ an "independent, impartial and neutral officer" to serve as ombudsman with "jurisdiction over problems or complaints about decisions, actions or inactions by ICANN, the Board of Directors or unfair treatment of a community member by ICANN, the Board or a constituency body."

importantly, because the contract was for a limited period of time (subject to extension by mutual agreement of NTIA and ICANN[50]), NTIA retained the option of re-opening the procurement and awarding the contract to some other party if it was unhappy with ICANN's performance.

NTIA's ability to re-open the IANA contract procurement was a serious and credible threat to ICANN's central role in DNS management. It was a serious threat because it would have had severe, and probably fatal, consequences for ICANN. ICANN's power ripples downward from the Root through the DNS hierarchy. Without the ability to specify the contents of the Root Zone File, ICANN could no longer guarantee TLD operators that their domains would continue to exist in the DNS; those TLD operators could therefore no longer guarantee to 2nd-level domain operators that *their* domains would continue to exist in the DNS; and so on down the line. And if that were the case, why would a TLD registry operator choose to comply with any ICANN policies or directives, or pay ICANN a fee?

It was a credible threat because replacement of ICANN through reprocurement of the IANA Functions Contract could be accomplished without a major disruption in universal name resolution or the specter of multiple, competing Roots. (See **Box 2.)** Because NTIA retained operational control of the Root, it would be able to find another party to exercise policy responsibility and then simply direct the party to whom it had delegated that operational control over the Root (*i.e.*, NSI/VeriSign) to implement the directives coming from that new entity, and to ignore those coming from ICANN.

So even though NTIA possessed no authority to shut ICANN down, or to order it to stop performing any DNS-related tasks, re-procuring the IANA contract would, for all intents and purposes, have accomplished that. Being able to credibly threaten to render ICANN entirely ineffective in DNS policy matters gave teeth to the possibility of a withdrawal of NTIA's recognition/endorsement, and it gave NTIA a significant measure of oversight control over ICANN's activities.

It is very difficult to know exactly how this oversight was exercised and exactly how significant it was for keeping ICANN in line, or how and how often it influenced the ICANN Board to forego actions that it might otherwise have been inclined to take. Like the proverbial Sword of Damocles, it can be performing its job very effectively even when it remains motionless. Observers of and participants in ICANN's activities over the years are, however, virtually unanimous in ascribing a special role for NTIA in ICANN oversight, and a special voice for the U.S. government in ICANN's affairs, deriving from the IANA contract and NTIA's reprocurement option.[51] There is little doubt that

---

50. NTIA and ICANN entered into contracts for the performance of the IANA functions in 2001, 2003, and 2006. The current contract was awarded to ICANN on July 2, 2012; the base period of performance for this contract is October 1, 2012, to September 30, 2015. The contract also provides for two option periods of two years each. If both option periods are exercised, the contract would expire on September 30, 2019. *NTIA Report*, *supra* note 32.

51. ICANN's Cross-Community Working Group writes, "NTIA's oversight is embodied in the IANA Functions Contract between the NTIA and ICANN. At the end of each contract term, the NTIA has had the option to issue a new RFP and potentially issue the contract to a party other than ICANN. The CWG believes that this has provided the NTIA with power (or 'leverage') to ensure that ICANN performs the IANA tasks described in the contract adequately. . . . Through its control of the Contract (which is of significant importance to ICANN), [NTIA] also has the ability to act as a 'backstop' to resolve accountability and performance issues involving ICANN outside of the performance of the IANA Functions. Ultimately, the NTIA has acted as the historical steward of the IANA Functions and by extension, the Domain Name System and the Internet." See https://community.icann.org/download/attachments/49351404/CWG%20IANA%20Issues%20for%20Independent%20Legal%20Advice.docx?version=1&modificationDate=1426157111000&api=v2.

See also Emma Llanso and Matthew Shears, *The IANA Transition in the Context of Global Internet Governance*, in William J. Drake and Monroe Price, eds., *Beyond NETMundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem* (Annenberg School of Communications at the University of Pennsylvania: August 2014) at 73: "The continuity and stability of the DNS are essential to the continuing success of the internet, and to the extent that NTIA's oversight has contributed to providing confidence in the system, this has been a crucial role. The idea of stewardship also has an additional dimension, related to institutional accountability for ICANN. The NTIA's ability to award – and possibly withdraw – the contract for the performance of the IANA functions has provided a mechanism that could counterbalance any actions by ICANN that might destabilize the DNS."

Mueller and Kuerbis, *Roadmap for globalizing IANA*, available at http://www.internetgovernance.org/wordpress/wp-content/uploads/ICANNreformglobalizingIANAfinal.pdf: "The IANA functions contract does far more than empower the US Commerce Department to authorize changes to the root zone. It regulates very detailed aspects of ICANN's behavior… and provides America with greater political influence over ICANN. Because the contract must be renewed every three years, the U.S. can modify the contract to shape ICANN's behavior, or threaten to award it to someone else…"

Box 3. The 2012 Re-Procurement

In November 2011, NTIA announced that it was re-opening the IANA Functions Contract to competitive bids for the period 2012-2015 [see http://www.ntia.doc.gov/files/ntia/publications/11102011_solicitation.pdf] because of concerns about loopholes in ICANN's Conflict of Interest Policy:

> "The Commerce Department... warned the organization [ICANN] that it needed to tighten its rules against conflicts of interest or risk losing a central role.... ICANN has come under heightened scrutiny because of an initiative to increase vastly the number and variety of available Internet addresses. Under the plan, which ICANN is putting into effect, hundreds of new 'top-level domains' are set to be created.... [T]he initiative has been cheered by companies that register and maintain Internet addresses. A number of current and former members of the ICANN board have close ties to such registrars or to concerns involved in other areas that stand to benefit from the expansion. 'ICANN must place commercial and financial interests in their appropriate context," said [Rod Beckstrom, former ICANN Chairman]... 'How can it do this if all top leadership is from the very domain-name industry it is supposed to coordinate independently? ... Eyebrows were raised last year when Peter Dengate Thrush, former chairman of ICANN and a fan of the domain name expansion, joined a company that invests in domain names." ("Ethics Fight Over Domain Names Intensifies," *New York Times* [March 18, 2012], available at http://www.nytimes.com/2012/03/19/technology/private-fight-at-internet-naming-firm-goes-public.html?_r=0.]

Shortly thereafter, ICANN reviewed, revised, and re-issued its Conflicts of Interest policy [see https://www.icann.org/en/system/files/files/summary-ethics-review-13may13-en.pdf and https://www.icann.org/news/announcement-2-2012-05-15-en] and the re-procurement was cancelled [see http://www.ntia.doc.gov/other-publication/2012/notice-internet-assigned-numbers-authority-iana-functions-request-proposal-rf].

the ICANN Board was aware of a line beyond which it could not go without risking NTIA's wrath. The one time during the past 15 years that NTIA actually invoked its re-procurement option and put the IANA Functions Contract out for bid certainly shows that ICANN took the threat seriously (see **Box 3** for more on the 2012 reprocurement) and a number of other incidents involving pressure from NTIA on ICANN give evidence of the special influence that the U.S. government had in ICANN's affairs.

But nobody can say for certain how ICANN would have behaved had NTIA not retained ultimate authority over the IANA Functions and the leverage that provided—precisely the question that now occupies center stage.

II. WHY DNS POLICY MATTERS

"The problem is how to prevent ICANN from using its authority [over] technical coordination of the Internet DNS... to expand its own powers beyond its limited mandate.... No one can seriously question [that] ICANN currently intrudes into areas beyond its technical mandate. ICANN's mission creep may result from confused thinking about Internet governance. Issues affecting ICANN, its performance, and decisions too often get conflated with the term 'Internet governance,' which comprises a broad array of issues, including legal and policy matters covering law enforcement, free speech, intellectual property, and the digital divide. But ICANN is not responsible for Internet governance, writ large."

Weber & Gunnerson, *Constitutional Solution*

"Control over the DNS confers substantial power over the Internet. Whoever controls the DNS decides what new families of "top-level" domain names can exist (e.g., new suffixes like .xxx or .union) and how names and essential routing numbers will be assigned to websites and other Internet resources. The power to create is also the power to destroy, and the power to destroy carries in its train the power to attach conditions to the use of a domain name.... In theory, the power conferred by control of the DNS could be used to enforce many kinds of regulation of the Internet [such as] content controls on the World Wide Web [WWW]... A more subtle, but already commonplace, use of the root authority involves putting contractual conditions on access to the root. ICANN has imposed a number of conditions on registrars and... registries on a take-it-or-be-delisted basis..."

Froomkin, *Wrong Turn in Cyberspace*

The IANA transition, proposed by NTIA in March 2014, involves, at bottom, simply allowing the IANA Functions Contract between NTIA and ICANN to expire on (or, at the latest, shortly after) its currently scheduled termination date of September 30, 2015.[52] That would entirely relinquish the U.S. government's procurement role in—and accompanying oversight over—the DNS and ICANN's performance of its DNS management functions.

At first glance, many people find it difficult to see why DNS management and DNS policy-making matter very much (and difficult to see, therefore, why the IANA Transition matters very much). But DNS policy—the seemingly simple matter of determining *which* domains are to be

52. *NTIA Announces Intent to Transition Key Internet Domain Name Functions* (March 14,2015), available at http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

available on the network, and *who* gets to operate those domains—necessarily encompasses difficult issues of privacy, property rights, free expression, and even national identity:

- Whether there is to be a .doctors top-level domain, and, if so, whether it will be reserved for licensed medical practitioners (and, if so, who decides which licenses are acceptable and which not?)[53];

- whether a *.berlin*, or *.amazon*, or *.champagne*, can be added to the Root (and, if so, who, if anyone, is "entitled" to operate that TLD?);

- whether a TLD registry operator may—or must?—register the 2nd-level domains *walmartsucks*[*.com*, or *.org*, or *.biz*, etc.] or *plannedparenthood*[*.com*, *.org*, *.biz*, etc.], or *bushforpresident*[*.com*, *.org*, *.biz*] (and who, if anyone, is entitled to operate those domains?);

- whether the Arabic, or Chinese, or Hebrew character sets can be used for domain names,[54] and, if so, whether TLD registries may (or perhaps must?) allow registration of لهذا المخطط قالأبو or 计划生育 or **מתוכננת הורות**[55] in addition to their English equivalents (and, again, if such registrations are permitted, who gets to operate those domains?);

- whether domain name registrars must obtain (and verify?) specific information about the identity of all registrants, and whether that information (or some subset) must be made publicly-accessible[56];

- whether a country-code TLD should be established for Palestine, or Kosovo, or Kurdistan[57];

- whether a registry operator who goes out of business or declares bankruptcy must transfer its subdomains to another registry operator;

- whether domain name holders can retain access to their domains if they want to switch registrars.

DNS policy questions like these (and the many others like them) are difficult, because while they all have a "technical" dimension, they do not have *only* a technical dimension; they invoke some important and deeply-held values far removed from the "merely" technical. How they are resolved will have an impact—small, but in the aggregate, not inconsiderable—on trade and commerce and competition, on intellectual property rights, on privacy, and on free expression.[58] And precisely because the DNS remains a single, unified system across the entire Internet, those impacts are felt globally.

---

53. See Hattem, *Fight Breaks Out over .doctor Websites* (March 25, 2015), available at http://thehill.com/policy/technology/236879-fight-breaks-out-over-doctor-websites; McCarthy, *Timeout, Time Lords: ICANN Says There is Only One Kind of Doctor* (March 15, 2015), available at http://www.theregister.co.uk/2015/03/15/icann_doctors/.

54. See Internationalized Domain Names, available at https://www.icann.org/resources/pages/idn-2012-02-25-en.

55. These names are all translations (according to Google Translate) of "planned parenthood" into Arabic, Chinese, and Hebrew, respectively.

56. ICANN policies regarding the information about registrants that must be made available in the publicly accessible "WHOIS" database have long been controversial. *See* https://www.icann.org/resources/pages/whois-policies-provisions-2013-04-15-en (compiling all ICANN WHOIS-related policies). *See also* Non-Commercial Users Constituency Report on the WHOIS Accuracy Pilot Study Report, available at http://forum.icann.org/lists/comments-whois-ars-pilot-23dec14/pdfoJR3FYgtyz.pdf, decrying the "divisive," "improper," and "dangerous" WHOIS policy developments.

57. *See* IANA Report on Request for Delegation of *.ps* Top-Level Domain (22 March 2000), available at https://archive.icann.org/en/general/ps-report-22maroo.htm.

58. There is a large literature on this subject; much of the scholarly work, for example, on "Internet governance" has focused on the ways in which the Internet's technical protocols and standards embody and affect non-technical norms and values, with the DNS often used as a prime illustration of the principle. See *The Internet and its Governance: A General Bibliography*, available at http://www.cairn.info/revue-francaise-d-etudes-americaines-2012-4-page-20.htm; Weber, *Shaping Internet Governance* (Springer Verlag, 2012); DeNardis, *Protocol Politics* (MIT Press, 2009); Nunziato, *Freedom of Expression, Democratic Norms, and Internet Governance*, 52 Emory L.J. 187 (2003); Drake, ed., *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (UN ICT Task Force Series 12, 2005).

That is enough, we think, to make the IANA Transition—proposing, as it does, to fundamentally re-structure the existing DNS policy-making apparatus—a significant event, one that needs more public attention, understanding, and debate than it has received up to now.

And as important as those questions are, the stakes involved in the IANA Transition reach considerably beyond the confines of the DNS and DNS policy. As the quotations at the beginning of this section suggest, control over the DNS can be leveraged and extended to cover a much broader range of Internet content and communication, raising very troubling questions of legitimacy and authority and power on the global network.

To understand how this can unfold, consider first the way that ICANN has put its "Uniform Dispute Resolution Procedure" (UDRP) into place. The UDRP was one of the ICANN's first policy initiatives,[59] and it was designed to respond to concerns about "cyber-squatting"—registering existing trademarks as domain names for the (sole) purpose of re-selling the name to the trademark owner.[60] The UDRP[61] is an ICANN-administered procedure under which a trademark holder can initiate a cyber-squatting complaint, heard (online) by an ICANN-accredited arbitrator. The arbitrator applies ICANN's rules for determining whether the offense has been committed,[62] and if the trademark owner prevails, the UDRP allows the arbitrator to cancel the offending domain name registration (or, alternatively, to transfer it to the trademark holder). This is accomplished by ordering the domain name registrar with whom the offending registration was placed to delete (or modify) the entry corresponding to that domain name, and to communicate that deletion/modification to the relevant TLD registry (so that the TLD's zone file will be modified accordingly). Compliance with these orders is assured by the requirement that all registrars must promise, in their "Registrar Accreditation Agreement" with ICANN, to comply with the UDRP arbitrator's order as a condition of obtaining ICANN's accreditation,[63] and by the requirement that that all TLD *registries* must promise, in their "Registry Agreement" with ICANN, to accept registrations only from ICANN-accredited registrars.

The UDRP is thus a mandatory proceeding, across the entire Internet, *one to which all domain name registrants, registrars, and registries in all TLDs under ICANN's control are subject*. (For an explanation of which TLDs are *not* under ICANN's control, see **Box 4**.) It addresses a very narrow slice of trademark law; it applies only to conflicts arising from the use of a trademark in a domain name; but with respect to that category of conflicts, it has proven to be an efficient and powerful global conflict-resolution system.[64] It can operate effectively at Internet scale; as of 2013, over 50,000 cases, from 175 countries, had been disposed of quickly and efficiently[65] (though whether they

59. ICANN adopted the UDRP in more-or-less its current form in August 1999. See *UDRP Timeline*, available at https://www.icann.org/resources/pages/schedule-2012-02-25-en.

60. See text at notes 17-18, above.

61. General information about the URDP can be found at https://www.icann.org/resources/pages/help/dndr/udrp-en.

62. The UDRP requires the trademark holder to show that the challenged domain name (a) is "identical or confusingly similar" to its trademark, and that whoever registered the domain name (b) "has no legitimate rights" to it and (c) acted "in bad faith." Evidence of "bad faith" includes circumstances indicating that the name was acquired "primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the . . . owner of the trademark or to a competitor of that complainant…" *See Uniform Dispute Resolution Policy*, available at https://www.icann.org/resources/pages/policy-2012-02-25-en.

63. See Section 3.8, Registrar Accreditation Agreement (obligating registrar to comply with UDRP), available at https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa.

64. See Christie, *Online Dispute Resolution – The Phenomenon Of The UDRP*, in Torremans (ed), *Research Handbook on Cross-Border Enforcement of Intellectual Property* (forthcoming 2015), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2433380.

65. *id*. "The system has shown it is capable of resolving cross-border IP disputes in a timely manner and at very low cost. It has delivered largely consistent outcomes across a huge volume of cases, while evolving to address scenarios that were unforeseen and unforeseeable at its implementation. It has… won international respect as an expedient alternative to judicial options for resolving trademark disputes arising across multiple national jurisdictions."

Box 4. The ccTLDs

Understanding the distinction between the "country-code" TLDs (ccTLDs) and the non-country-code TLDs (the so-called "generic" TLDs, or "gTLDs") is critical for understanding the scope of ICANN's power to set DNS policy.

Country-code TLDs, as their name implies, represent individual nations, and are identified by the standard two-letter country codes defined by the International Standards Organization (in ISO-3166, *see* http://www.iso.org/iso/country_codes.htm). For example, *AU* for Australia, *EC* for Ecuador, *HU* for Hungary, etc. Many of these ccTLDs have become quite popular in recent years, such as *.tv* and *.fm*, which are the country codes for Tuvalu and the Federation of Micronesia, respectively. At present, approximately 130 million of the 290 million registered domain names (roughly 45 percent) are within the ccTLDs.

ICANN policies (including the UDRP) are not binding on ccTLD registry operators, because the vast majority of the more than 200 ccTLDs have no contractual or other formal relationship with ICANN at all. Unlike gTLD registries, each of whom must execute ICANN's Registry Agreement and agree to be bound by ICANN policies as a condition of being placed into the Root Zone File, ICANN will recognize a ccTLD registry in the absence of any formal contractual relationship with it.

ICANN's relationship with the ccTLDs has undergone considerable modification over the years. Delegation decisions—deciding who gets to operate the authoritative registry database for each ccTLD in cases of conflicting claims—can be (and on occasion have been) difficult and controversial, particularly in situations involving political instability. (See http://ccnso.icann.org/workinggroups/foi-final-07oct14-en.pdf.) ICANN policy with respect to "recognizing" ccTLDs is set forth in two basic documents: Jon Postel's 1994 framework document (RFC 1591, see http://www.isi.edu/in-notes/rfc1591.txt), and ICANN's Principles And Guidelines For The Delegation And Administration Of Country Code Top Level Domains, prepared by ICANN's Government Advisory Committee and adopted by the ICANN Board in 2005 (see https://archive.icann.org/en/committees/gac/gac-cctld-principles.htm). The basic framework establishes local government control over the conduct and the policies of each ccTLD.

have done so fairly is open to dispute[66]). It is impossible to imagine any set of national courts managing to process this volume of litigation as quickly, and at such low cost. It solves two of the most difficult problems surrounding the enforcement of cross-border legal rights and obligations: the problem of choice of law (*i.e.*, determining whose substantive rules apply to conflicts involving persons from different countries), and the problem of judgment enforcement (*i.e.*, obtaining enforcement of a legal judgment issued in one jurisdiction against a wrongdoer located in a different jurisdiction). Under the UDRP, one set of rules—ICANN's—applies to all disputes, and because the rules are enforced through the domain name databases themselves, they can be effective no matter where anyone involved in the dispute—the complaining trademark owner, the domain name registrant, the registrar who sold the domain name, or the registry of the TLD in question—is located.

It is so powerful and efficient, in fact, that it makes a tempting model for those who would like to see ICANN use its contractual leverage over the DNS to enforce other rights, private or public, and to use domain name revocation as a remedy for other perceived harms and other objectionable expression. Copyright holders, for example, have very publicly called upon ICANN to assist them in their decades-long battle against file-sharing websites by setting up a copyright version of the UDRP; trademark interests have called upon ICANN to broaden the scope of the UDRP to cover not only infringing *domain*

66. Compare Christie's treatment of the UDRP, *id.*, with Komaitis, *The Current State of Domain Name Regulation: Domain Names as Second Class Citizens in a Mark-Dominated World* (Routledge 2012) (UDRP is "based on illegitimate grounds, its procedures are substantially flawed and unfair, it restricts the rights of domain name registrants, and it is crowded with examples of inconsistent and biased decisions"), and Geist, *Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, available at http://aix1.uottawa.ca/~geist/geistudrp.pdf.

names, but any infringing trademark uses; others have proposed a more active role for ICANN in combatting the distribution of child pornography or other objectionable or unlawful content, or in helping to police for Internet sites from which "cyber-attacks" of one kind or another have been launched.[67]

Clearly, whoever controls the DNS will inevitably be subject to intense pressure, from many directions, public and private, to use this leverage to broaden the scope of its enforcement powers, to reach elements of Internet communications—message *content*—beyond those elements necessary for the smooth functioning of the DNS and its narrow name-resolution function. But using control over fundamental Internet technical infrastructure to regulate activities taking place at a different level in the protocol stack in this way is deeply troubling, for many reasons.[68] ICANN has not been constituted and organized for the purpose of setting global copyright (or consumer protection, or fraud, or pornography, or trademark) policy, and an institution that is well-designed for the task for which it was constituted would hardly be well-suited for these other functions. ICANN officials have, to be fair, publicly disclaimed any interest in having the corporation take on a broader, more generalized global law-enforcement role of this kind. A number of the corporation's recent actions, however, suggest otherwise. (See **Box 5** for more on ICANN as a global law enforcer.)

So this, too, is part of what is at stake in DNS policy-making and in the IANA Transition. Freed from US government oversight, what is to prevent ICANN—or whoever controls this critical Internet resource—from inserting itself into global law-enforcement/governance role far removed from its core commitment to ensuring that the DNS runs smoothly and efficiently?

---

67. See Internet Governance Project, *What to Do About ICANN: A Proposal for Structural Reform* (2005), available at http://www.internetgovernance.org/pdf/igp-icannreform.pdf (describing ICANN's forays into competition policy, rate regulation, intellectual property policy, freedom of expression, and taxation); Weber & Gunnerson, *Constitutional Limitations*, *supra* note 39, at 63-9 (describing ICANN "mission creep" into areas outside of its technical mandate).

With respect to pressure on ICANN to play a more aggressive role in copyright and trademark enforcement, see Post, *ICANN, Copyright Infringement, and the "Public Interest,"* (March 9, 2015), available at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/03/09/icann-copyright-infringement-and-the-public-interest/; RIAA letter to ICANN Board (March 5, 2015), available at https://www.icann.org/en/system/files/correspondence/riaa-to-icann-05mar15-en.pdf ("ICANN recently passed a resolution that...provides that a 'Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from...piracy, trademark or copyright infringement..., and providing...consequences for such activities including suspension of the domain name.'"); *MPAA Pushes for ICANN Policy Changes to Target 'Pirate Domains'* (Feb. 27, 2015), available at https://torrentfreak.com/mpaa-pushes-icann-policy-changes-target-pirate-domains-150227/; *2013 Joint Strategic Plan On Intellectual Property Enforcement* at 36 ("[IPEC] will continue to facilitate and encourage dialogue among different private sector entities that make the Internet function, which may include domain name registries and registrars"), available at https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf; United States Trade Representative, *2014 Out-of-Cycle Review of Notorious Markets*, at 10-12 (March 5, 2015) (identifying domain name registrars as a "new issue focus" in the USTR's "Special 301" process for targeting notorious global markets for piracy and counterfeiting).

68. Objections to using the technological infrastructure to enforce legal norms and obligations were highlighted in the controversy surrounding the introduction of the Stop Online Piracy Act (SOPA) and the PROTECT IP Act in 2010-11. See Lemley et al., *Don't Break the Internet*, Stanford Law Review Online (Dec. 19.2011), available at http://www.stanfordlawreview.org/online/dont-break-internet (noting that the bills' use of "mandated court-ordered filtering" through the DNS represented an "unprecedented, legally sanctioned assault on the Internet's critical technical infrastructure" and "threatens the fundamental principle of interconnectivity that is at the very heart of the Internet"); Crocker et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," available at https://cdt.org/files/pdfs/Security-Concerns-DNS-Filtering-PIPA.pdf.

See generally Benkler et al., *Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295953 (analyzing and mapping the extraordinary public discussion and debate surrounding the two bills).

Box 5. ICANN as Global Law Enforcer

In 2013, as it was opening up the Root to several hundred new TLD registries, ICANN unilaterally—at the instigation, apparently, of the Government Advisory Committee, without going through the mandated Consensus Policy Development Process described above—revised its Registry Accreditation Agreement for all new registries. A new "Public Interest Commitment" requirement was inserted requiring, among other things, that registries "flow-through" to all registrars the requirement that they include a provision in their contracts with registrants that prohibits the registrants

> ". . . from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law . . ."

Registrars must provide for "consequences for such activities, *including suspension of the [registrant's] domain name."* And registries and registrars also must agree that if ICANN, in its sole discretion, determines that they are not complying with these new requirements, they will "implement and adhere to any remedies ICANN imposes" for such non-compliance, "including termination" of their registry or registrar accreditation (which would effectively end that part of their business operations).

On the surface, it looks harmless enough; why shouldn't anyone wishing to register *fabulouscellphone.app*, or *washingtonpost.blog*, or *dewey-cheatem-and-howe.attorney*, or any other 2nd-level domain in these TLDs, promise not to engage in "piracy" or "fraud," or any activity "contrary to applicable law"? Who wouldn't promise such a thing?

On the other hand, it means registries and registrars will henceforth, at the risk of losing their position in the DNS, have to satisfy ICANN that they are taking appropriate steps to suspend domains associated with end-users who engage in "fraud" or "deceptive practices" or "piracy" or any activity "contrary to applicable law." ICANN has already set up a new dispute resolution apparatus—the "Public Interest Commitment Dispute Resolution Procedure" or "PICDRP"—to assist in determining whether registries and registrars are complying with their Public Interest Commitments, and ICANN retains "sole discretion" to decide whether the Operator is or is not compliant, and to decide on the appropriate remedy "which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement."

What kinds of procedures will satisfy ICANN that "appropriate" steps are being taken? And what does any of this have to do with the purposes for which ICANN has been constituted and organized—assuring uniformity and stability of the DNS, and making sure that the Internet's system for resolving names into IP Addresses continues to function smoothly?

III. THE IANA TRANSITION: OPPORTUNITIES

The risks posed by the IANA transition are thus serious and substantial—but at the same time, it presents a significant, and possibly historic, opportunity for the United States and for the global community of Internet users. It is the logical culmination of the sequence initiated in the '98-'99 transition. From the very beginning, the DNS White Paper articulated the position that the U.S. government's continuing role in procuring the IANA functions would be temporary,[69] stressing that NTIA intended "only to procure the IANA functions services until such a time as the transition to private sector management of the DNS was complete."[70] Although we believe that the U.S. government has handled the evolution of the Internet and its governance systems well so far, the justifications for a special role for the U.S. government in managing that evolution are considerably weaker in 2015 than they were in 1998,[71] as a consequence of both the Internet's vastly expanding global reach and of questions about the U.S. government's ability to claim any kind of neutral "stewardship" role for itself with respect to Internet affairs.[72] The 2013 Snowden disclosures, among their many economic, political, and cybersecurity-related ramifications,[73] exacerbated longstanding tensions in the global Internet governance community relating to ICANN's special relationship with the United States, and there is considerable evidence that if NTIA had not voluntarily decided to begin the transition, other Internet stakeholders—including important elements of the

69. Recognizing the changing times, the DNS White Paper acknowledged that "the Internet is rapidly becoming an international medium for commerce, education and communication" and that "[t]he pressures for change are coming from many different quarters." *DNS White Paper.*

70. *NTIA Report*, *supra* note 32.

71. While some of these tensions date back to the very creation of ICANN in 1998, they began to emerge most starkly in 2003 prior to the World Summit on Information Society (WSIS). As Milton Mueller explains:

> "It was a truly global regime in which policy-making authority was delegated to transnational private actors under the supervision of the United States, and other governments were relegated to an advisory role in a 'Governmental Advisory Committee' (GAC). Setting aside the question whether this is a good or a bad governance model, in the fall of 2003 the catalyst of conflict at WSIS was simply how thoroughly it deviated from the multilateral agreements among sovereign nations, which many states took as the norm for global governance... Other aspects of U.S. dominance on the Internet, such as concentrated technical expertise and its role as a hub for global connectivity were too intangible or diffuse to be changed by policy or used as a target. It was therefore logical and predictable that ICANN became the target of a multilateral, intergovernmental process focused on Internet governance." Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010) at 63-64.

These tensions have not been diffused in recent years. "While some progress [has been] made in acknowledging the importance of the distributed and bottom-up internet ecosystem and beginning to address internet policy and governance questions, the issue of the US government's role in "controlling the root" via ICANN and the IANA functions was – and continues to be – a sticking point." Llanso and Shears, The IANA Transition in the Context of Global Internet Governance, *supra* note 51, at 74.

72. See, e.g., Milton Mueller, *Do the NSA Revelations Have Anything to Do With Internet Governance?*, Internet Governance Project (February 19, 2014), available at http://www.internetgovernance.org/2014/02/19/do-the-nsa-revelations-have-anything-to-do-with-internet-governance/. (Mueller argues that the NSA disclosures "threaten... in a very fundamental way the claim that the US had a special status as neutral steward of Internet governance.") In fact, the idea of "stewardship" itself has become increasingly complex in recent years. See, e.g., discussion of this question in Llanso and Shears, "The IANA Transition in the Context of Global Internet Governance," at 72-73.

73. For a full discussion of the impact of the Snowden revelations on the U.S. economy, foreign policy, and cybersecurity, see Danielle Kehl et al., *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity,* New America's Open Technology Institute (July 28, 2014), available at http://www.newamerica.org/oti/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-and-cybersecurity/.

technical community, foreign governments, and ICANN itself—would have tried to force its hand.[74] In October 2013, only a few months after the initial Snowden leaks, the heads of a number of key non-governmental Internet governance organizations, including ICANN, IETF, and the five RIRs, publicly voiced their concerns about the United States' waning credibility as the steward of the IANA functions in the Montevideo Statement on the Future of Internet Cooperation. The statement expressed "strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance" and "called for accelerating the globalization of ICANN and Internet Assigned Numbers Authority (IANA) functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing."[75]

The IANA transition also has important symbolic significance, a formal recognition by the United States that the Internet—which the United States government helped usher into existence 30 years ago—is now truly a *global* public trust, and that the Internet's core infrastructure is not the special purview of any one country's exclusive jurisdiction, but rather needs to evolve in ways that benefit all users, world-wide. Since 2004, roughly 1.8 billion people have come online,[76] with another 500 to 900 million people predicted to join the online population by the year 2017.[77] The vast majority of these new Internet users reside outside the United States, in Europe as well as in countries across the Global South. Moreover, in parallel to the growth of the network itself, the ecosystem of multistakeholder (and multilateral) Internet governance organizations has also grown exponentially. What was once a handful of technical organizations and policymaking forums has transformed in the past decade into a sprawling and decentralized system of both regional and global institutions and convenings.[78] As both the network and the systems that govern it have grown and evolved in recent years, it has become fairly clear that the governments of the world have a claim—but no *special*

---

74. Historically, many countries have objected to the way ICANN operates and its ties to the U.S. government. In 2011, for example, India proposed the creation of a UN Committee for Internet-Related Policies (CIRP) that would have placed many of the policymaking functions performed by ICANN and issues discussed at the Internet Governance Forum under the purview of a 50-country government committee with four advisory groups (for civil society, the technical and academic community, businesses, and international and intergovernmental organizations) to "advise and assist" them—an inversion of the ICANN model. *See* "India's Proposal for a United Nations Committee for Internet-Related Policies (CIRP)," Statement by Mr. Dushyant Singh, Honorable Member of Parliament, India, Sixty Sixth Session of the UN General Assembly (October 26, 2011) available at http://itforchange.net/sites/default/files/ITfC/india_un_cirp_proposal_20111026.pdf. (One of the proposed activities in the CIRP's mandate would be to "[c]oordinate and oversee the bodies responsible for technical and operational functioning of the Internet, including global standards setting"). Efforts have also been made to bring some or all of the tasks related to the management of the DNS under the oversight of the International Telecommunication Union, the UN specialized agency responsible for the interoperability of global telecommunications networks.

75. See *Montevideo Statement on the Future of Internet Cooperation* (October 7, 2013), available at https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm; *also see* NETmundial Multistakeholder Document (April 24, 2014), available at http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf:

> "It is expected that the process of globalization of ICANN speeds up leading to a truly international and global organization serving the public interest with clearly implementable and verifiable accountability and transparency mechanisms that satisfy requirements from both internal stakeholders and the global community" and "This transition should be conducted thoughtfully with a focus on maintaining the security and stability of the Internet, empowering the principle of equal participation among all stakeholder groups and striving towards a completed transition by September 2015."

76. "World development indicators," World Bank, 2013 estimates, sourced from the International Telecommunication Union (ITU), "World telecommunication/ICT development report" and database, and World Bank estimates.

77. *Offline and Falling Behind: Barriers to Internet Adoption*, McKinsey & Company (September 2014), available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/offline_and_falling_behind_barriers_to_internet_adoption.

78. In 2005, the United Nations Working Group on Internet Governance (WGIG) broadly defined Internet governance as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." *Report of the Working Group on Internet Governance* (June 2005), available at http://www.wgig.org/docs/WGIGREPORT.pdf at 4. Today, different aspects of Internet governance are discussed by a wide range of organizations and at various events events—everything from technical and policymaking organizations which meet regularly (like ICANN and IETF) to periodic convenings (like the annual Internet Governance Forum (IGF)) and intergovernmental summits (like the International Telecommunication Union (ITU) and other UN bodies).

claim—to direct that evolution. Even members of the United States Congress in 2012 unanimously agreed that there should be no government control, nor privileged role for governments of the world, in the operation of the multistakeholder model of Internet governance.[79] The IANA transition is the opportunity to show that we mean what we say.

A strong, consensus-based, non-governmental, multi-stakeholder institution at the policy-making center of the DNS is also likely to be the best way to ensure that the Internet infrastructure remains free from undue governmental influence—especially from foreign governments whose views regarding free and open expression on the Internet are at best less clear than, and at worst inimical to, those of the United States.[80] The growing opposition from the international community over the past several years about NTIA's privileged role in ICANN oversight has created a perceived imbalance that plays into the hands of governments seeking to undermine the multistakeholder model of Internet governance. If the transition succeeds, it would alleviate some of this international pressure, which could help the United States and its allies in their ongoing efforts to prevent government overreach on other issues of Internet governance.

By initiating the transition voluntarily, NTIA has been able to maintain a high level of credibility—which is especially remarkable during a time of overall erosion of trust in the United States in the Internet governance space—and is positioned firmly to reject any transition proposals that fail to meet the criteria it has laid out or that might undermine the free and open Internet. By contrast, any attempt to delay or interfere with the transfer of IANA oversight to the global multistakeholder community could further empower critics like China and Russia, who have long favored a governmental or intergovernmental approach to Internet governance and would relish an opportunity to claim authority over the IANA functions through the UN's International Telecommunication Union or another government-dominated entity. The better strategy is to focus efforts on ensuring that the transition is carefully planned with robust accountability mechanisms, rather than attempting to hold on to the last vestige of U.S. oversight of the Internet for as long as possible. Even members of the U.S. Senate were fairly unanimous during a February 2015 hearing on the IANA transition in asserting that there should be no government control in the operation of this part of the Internet ecosystem.[81]

Getting the transition right has broad implications for the evolution of the Internet governance system. Its success—or failure—could have a significant impact on the shifting dynamics of the global debate more broadly, affecting both the United States' credibility and the weight of its support for the multistakeholder model. Moreover, the process itself could inform the evolution of decision-making structures in other key Internet governance institutions. As Emma Llanso and Matthew Shears from the Center for Democracy and Technology explain: "The transition presents an opportunity to develop praxis on identifying

79. H. CON. RES. 127/S. CON. RES. 50, which recognizes that "given the importance of the Internet to the global economy, it is essential that the Internet remain stable, secure, and free from government control" and "this and past Administrations have made a strong commitment to the multistakeholder model of Internet governance and the promotion of the global benefits of the Internet." The resolution was passed by both the House and Senate prior to the International Telecommunication Union's 2012 World Conference on International Telecommunications. For the full text of the resolution, see https://www.govtrack.us/congress/bills/112/hconres127/text.

80. *See, e.g.*, stakeholder responses in *NTIA Report*, *supra* note 32, at pp. 6-9.

81. "Hearing: Preserving the Multistakeholder Model of Internet Governance," U.S. Senate Committee on Commerce, Science, and Transportation (February 25, 2015), available at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=683924ae-83d7-4bf4-922a-cdecb9556ba9. For more discussion of the hearings, see David Post & Danielle Kehl, *Senate Hearings on the IANA Transition Provide Troubling Insight Into Policymakers' Priorities*, New America's Open Technology Institute (March 2, 2015), available at http://www.newamerica.org/oti/senate-hearings-on-the-iana-transition-provide-troubling-insight-into-policymakers-priorities/.

diverse stakeholders who can and should contribute to governance processes, conducting effective outreach, and bringing those stakeholders into a governance discussion typically dominated by technical considerations in a way that enables them to meaningfully contribute."[82] If done correctly, the transition process could bolster the multistakeholder approach to Internet governance and offer valuable lessons to inform a broader range of governance decisions.

82. Llanso and Shears, *The IANA Transition in the Context of Global Internet Governance*, *supra* note 51, at 77.

CONCLUSION

The IANA transition is an important moment in Internet history and, therefore, in the history of human communication. NTIA's proposal has been met, thus far, with considerable support from a broad range of Internet stakeholders in the private sector, civil society, foreign governments, and the technical community,[83] a broad developing consensus that it is "time to get the [U.S.] government out of the Internet governance business," as former FCC Commissioner Robert McDowell put it.[84]

We share that enthusiasm. A successful transition will establish a vitally important principle for global network policy: that critical Internet resources can and should be managed by the global Internet community, outside of the confines of existing multi-lateral governmental institutions. A successful transition will also—like the '98-'99 transition—be invisible to the vast majority of Internet users; the DNS need not and should not command a great deal of the public's attention if it is running smoothly in the background and in good hands.

On the other hand, if it is unsuccessful—if the system fragments, or is otherwise mis-managed, or used to impose regulation on a broader range of Internet activity and communication—the consequences for Internet use and Internet users worldwide could be severe, and even disastrous.

We are enthusiastic because we believe that the transition can be managed so that the opportunities it presents are not squandered, and that the risks it poses do not come to pass. NTIA has laid out five basic principles for the transition. An acceptable structure or mechanism to replace NTIA oversight and take over the IANA functions must:

1. "support and enhance the multistakeholder model";
2. "maintain the security, stability, and resiliency of the Internet DNS," including preservation of the "decentralized distributed authority structure of the DNS so as to avoid single points of failure, manipulation, or capture";
3. "meet the needs and expectation of the global customers and partners of the IANA services";
4. "maintain the openness of the Internet," including the "neutral and judgment-free administration of the technical DNS and IANA functions [which] has created an environment in which the technical architecture has not been used to interfere with

83. See *NTIA Report*, *supra* note 32 (describing developing consensus); "Internet Technical Leaders Welcome IANA Globalization Process," ICANN (March 14, 2014), available at https://www.icann.org/news/announcement-2-2014-03-14-en; Testimony of the Honorable Lawrence E. Strickling, Assistant Secretary for Communications and Information, NTIA, before the U.S. House of Representatives Committee on Energy and Commerce's Subcommittee on Communications and Technology (April 2, 2014), available at http://www.ntia.doc.gov/speechtestimony/2014/testimony-assistant-secretary-strickling-hearing-ensuring-security-stability-re; Remarks by Lawrence E. Strickling, State of the Net Conference (January 27, 2015), available at http://www.ntia.doc.gov/speechtestimony/2015/remarks-assistant-secretary-strickling-state-net-conference-1272015.

84. There are, however, a number of prominent dissenting voices, including some in Congress. In April 2014, for example, Representative John Shimkus introduced the "Domain Openness Through Continued Oversight Matters (DOTCOM) Act," which would prohibit NTIA from completing the transition until the completion of an impact assessment by the Government Accountability Office (GAO), a process that could take up to a year. Other legislative attempts have aimed at restricting NTIA from using any Congressional appropriations to fund work on the transition—one of which was successfully added to the "Crominbus" appropriations bill in December 2014. For a good overview of the political tensions, see Jonah Force Hill, *No Guarantees on the ICANN Transition*, Global Policy Journal (September 18, 2014) available at http://www.globalpolicyjournal.com/blog/18/09/2014/no-guarantees-icann-transition.

the exercise of free expression or the free flow of information."

And it (5) must not "replace[] the NTIA role with a government or an inter-governmental organization solution."[85]

It is, we believe, the right place to begin, and we are optimistic that a transition plan can be devised and implemented that meets these goals.[86] The devil, however, is in the details, and it is of paramount importance for the preservation of a free and open Internet that we get those details right. We will examine those questions in the next paper in this series.

85. *NTIA Report, supra* note 32; *IANA Functions and Related Root Zone Management Transition Questions and Answers*, National Telecommunications and Information Association (March 18, 2014), available at http://www.ntia.doc.gov/other-publication/2014/iana-functions-and-related-root-zone-management-transition-questions-and-answ.

86. NTIA has directed ICANN to convene the transition process, leading to the creation of an IANA Stewardship Transition Coordination Group (ICG) with representation from over a dozen Internet stakeholder communities, and a somewhat bewildering array of transition proposal components are now being prepared. For more information, see https://www.icann.org/stewardship/coordination-group and https://www.icann.org/stewardship-accountability#processes.