The Origins of ccTLD Policymaking

Peter K. Yu
peter_yu@msn.com

Follow this and additional works at: https://scholarship.law.tamu.edu/facscholar
Part of the Intellectual Property Law Commons, and the Internet Law Commons

Recommended Citation
Available at: https://scholarship.law.tamu.edu/facscholar/546

This Article is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Texas A&M Law Scholarship. For more information, please contact aretteen@law.tamu.edu.
A long time ago in a galaxy not so far away, there was a decentralized global network of computers. These computers shared information with each other regardless of how far apart they were and whether there was any direct line of communication between them. In the very beginning, this network was used exclusively by government and military agencies, educational and research institutions, government contractors, scientists, and technology specialists. Instead of the domain names we use today, such as "www.amazon.com," users typed in numeric addresses, such as
"123.45.67.89," and, later, host names to send information to other computers.\(^2\)

This network soon expanded, and domain names became a practical necessity.\(^3\) There are at least two reasons. First, alphanumeric texts are generally easier for humans to remember than numeric addresses. Second, as Internet traffic increases and computer systems are reconfigured, the computer server used for a particular Web site may change from time to time. In fact, some busy Web sites might use multiple servers, requiring them to take turns to address requests directed to a single domain name. While the Web site owner (or his or her technical staff) might know internally to which numeric address the Web site corresponds at a particular moment, the general public does not. Domain names are therefore needed for identification purposes.

Although domain names are easy for humans to remember, computers do not understand these catchy names. Instead, computers have to "translate" these names back to numeric addresses before locating the information the users requested. To maximize efficiency and minimize storage, the Domain Name System ("DNS") was designed as a hierarchy, like a pyramid. To "resolve" a domain name, the computer issues a query to the name server at the bottom of the hierarchy. If the computer fails to obtain an answer, it will move up the hierarchy. If the computer still does not obtain an answer, it will continue to move up the hierarchy until it finally succeeds.

At the apex of this hierarchy is a set of thirteen legacy root zone servers, which identify the name servers storing the root zone files for all the top-level domains, including both the generic do-

---


\(^3\) See MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 39-40 (2002) [hereinafter MUELLER, RULING THE ROOT]. As Craig Partridge, the chief scientist of BBN Technologies, recalled: "When we got to about two thousand hosts, that's when things really started to come apart. Instead of having one big mainframe with twenty thousand people on it, suddenly we were getting inundated with individual machines, and everyone wanted to be named Frodo." HAFNER & LYON, supra note 1, at 252.
mains—such as ".com," ".net," or ".org"—and country-code top-level domains ("ccTLDs")—such as ".cn" (China), ".fr" (France), and ".tv" (Tuvalu). Each of these servers is assigned a letter from A to M. For example, the Internet Systems Consortium operates the "F Root Server," and the server in London is called the "K Root Server." More than three-quarters of these servers are located in the United States, and the rest are found in Japan, Sweden, and the United Kingdom.

To perform its identifying function, a domain name needs to be unique. Thus, all root zone files must contain identical data. As a past legacy, the database in the A Root Server, which the Internet Corporation for Assigned Names and Numbers ("ICANN") currently controls by virtue of its contract with the U.S. Department of Commerce ("DoC"), is considered authoritative. The other root servers merely copy this root zone file to their servers.

Due to this hierarchy and the lucrative market created by the sale of domain names, there has been an ongoing power struggle over the control of the DNS and authority to delegate and administer ccTLDs. This Essay recounts the story of this struggle, tracing how ccTLD policymaking has been transformed from ad hoc, informal coordination to international, contract-based governance. The Essay also discusses the various major players in the ccTLD debate: ICANN, the Internet Assigned Numbers Authority ("IANA"), ccTLD managers, national governments, the Interna-

---

4 For the location of these root servers, see Internet Domain Names: Hearings Before the Subcomm. on Communications of the Senate Comm. on Commerce, Sci., and Transp., (107th Cong. 2001) (statement of Michael M. Roberts, President and CEO, ICANN), available at http://www.icann.org/correspondence/roberts-testimony-14feb01.htm. To enhance Internet response times and reduce the vulnerability of the Internet root server system to malicious attacks, the Internet Systems Consortium recently deployed new root server sites around the world. In 2003, ISC deployed seventeen new F root server sites around the world. ISC plans to deploy twelve additional sites in 2004. See Press Release, Internet Systems Consortium, APNIC and APJII Install First Root Nameserver in Jakarta, Indonesia, at http://www.isc.org/about/press/?pr=2004072700 (July 27, 2004). The more recent server sites are located in Brisbane, Australia; Toronto, Canada; Monterrey, Mexico; Lisbon, Portugal; Tel Aviv, Israel; and Jakarta, Indonesia.

5 See ICANN, ICP-3: A Unique, Authoritative Root for the DNS (July 9, 2001), available at http://www.icann.org/icp/icp-3.htm (noting that "[f]rom the inception of the DNS, its most fundamental design goal has been to provide the same answers to the same queries issued from any place on the Internet"). But see infra note 83 (discussing alternative root servers).
tional Telecommunication Union ("ITU"), and the World Intellectual Property Organization ("WIPO").

The ccTLD policymaking story began when scientists, including Jon Postel and Paul Mockapetris, developed the DNS in 1983.6 Under a contract with the U.S. government, Postel, and later IANA, managed the DNS and delegated ccTLDs to foreign managers.7 The first ccTLD, ".us," was created and delegated in March 1985.8 Two other delegations, ".uk" (United Kingdom) and ".il" (Israel), followed in the same year.

At that time, very few countries were connected to the Internet backbone, and most of them did not need a ccTLD. Even when they needed one, ccTLD delegations usually fell into the hands of university computer science departments or educational and research networking organizations, rather than government agencies or organizations that historically provided postal, telephone, or telegraph services.9

From 1985 to 1993, Postel delegated ccTLDs on a first-come, first-served basis. Using the notion of a "responsible person," Postel required very limited basic administrative criteria before he delegated a ccTLD. As he wrote, the person in charge of assigning second-level domain names "is generally the first person that asks for the job (and is somehow considered a 'responsible person')."10

To avoid political problems, Postel used the ISO 3166-1 country codes to define what entity would warrant a ccTLD.11 Because these codes were provided by the International Organization for Standardization, an international association of national standard-

---


8 For the dates of ccTLD delegations, see DNSO, ICANN, History of the Internet: ccTLDs in Chronological Order of Top Level Domain Creation at the InterNIC, at http://www.cctld.dns.org/ccwhois/cctld/ccTLDs-by-date.html (Nov. 7, 2002).

9 See Mueller, Ruling the Root, supra note 3, at 88.

10 See id. at 88-89 (quoting Postel).

setting bodies, their objectivity successfully shielded IANA from the political pressure of deciding what was and was not a country.

Although the use of ISO 3166-1 codes appears systematic and well planned, the ".uk" ccTLD betrayed the ad hoc nature of early ccTLD policymaking. The ISO 3166-1 country code for the United Kingdom is ".gb" (for "Great Britain"); yet, Postel assigned " .uk" as the country's ccTLD. Moreover, during a brief period in 1996, IANA delegated codes under the ISO 3166 reserve list, which the ISO 3166 Maintenance Agency reserved specifically for postal purposes.

Notwithstanding the ad hoc nature of ccTLD delegation, conflicts rarely arose. Even if they did, when two parties competed for the same ccTLD, Postel usually succeeded in using subtle pressure to induce disputing parties to settle the issue before delegation. As IANA reasoned in a later document, dispute resolution "is usually a long drawn out process, leaving at least one party unhappy, so it is far better when the parties can reach an agreement among themselves."

By the early 1990s, the Internet had exploded onto the world stage. As more countries became connected and as national governments (and private companies) began to realize the full socio-economic potential of a ccTLD, requests for ccTLD delegations increased substantially. The number of delegations went from forty-six in 1990 to 108 in 1993. By the mid-1990s, IANA had delegated the ccTLDs for virtually all existing countries, including those with very limited Internet access.

With the increase in interest in ccTLDs, a more explicit delegation and administration policy was in order. In March 1994, Postel published RFC 1591, which described his delegation and

---

13 Examples of these ccTLDs include " .ac" (for Ascension Island), " .gg" (for Guernsey), " .im" (for the Isle of Man), and " .je" (for Jersey). See Kim G. von Arx & Gregory R. Hagen, Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control, 9 RICH. J.L. & TECH. 4 § 40 n.86 (2002), available at http://www.law.richmond.edu/jolt/v91/article4.html; see also RFC 3071, supra note 12, at 6 (recognizing that these exceptions "are arguably, at least in retrospect, just mistakes").
14 MUELLER, RULING THE ROOT, supra note 3, at 89.
16 MUELLER, RULING THE ROOT, supra note 3, at 127.
administration policy. It stated, first and foremost, that there must be a designated manager for supervising the ccTLD name space, and the administrative contact must reside in the country. Because the manager is the "trustee" for both the nation and the global Internet community, the manager must be equitable to all those who request a domain name. In addition, the manager must do a "satisfactory job" of operating the DNS service for the domain, and "significantly interested parties" in the domain must agree that the delegation is appropriate.

Moreover, RFC 1591 ensured that IANA would strictly adhere to the ISO 3166-1 list as the basis of ccTLD delegations. As the document stated, "IANA is not in the business of deciding what is and what is not a country." Should a dispute arise, IANA would "try to have any contending parties reach agreement among themselves, and generally take no action to change things unless all the contending parties agree." IANA would only intervene "in cases where the designated manager has substantially misbehaved," although RFC 1591 did not indicate what constituted misbehavior or substantial misbehavior.

---

17 Jon Postel, Domain Name System Structure and Delegation (Network Working Group, Request for Comments No. 1591) (Mar. 1994) [hereinafter RFC 1591], available at http://www.rfc-editor.org/rfc/rfc1591.txt. RFC stands for "Request for Comments." Although RFCs were sometimes published in final form, they generally "were intended to be an informal fast distribution way to share ideas with other network researchers." Leiner et al., supra note 1. As Don Mitchell described, the RFC process was a "sometimes brutal process of someone advancing an idea and everyone beating on it until the group consensus was that it would work." Mueller, Ruling the Root, supra note 3, at 94 (quoting interview with Don Mitchell). Once a consensus was achieved, the RFC would become an Internet standard until it was replaced by another RFC. For a detailed discussion of RFCs and Internet standard-making, see generally A. Michael Froomkin, Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace, 116 Harv. L. Rev. 749 (2003) [hereinafter Froomkin, Habermas@Discourse.Net]. As RFC 1718 stated: "There are . . . two special sub-series within the RFCs: FYIs and STDs. The For Your Information RFC sub-series was created to document overviews and topics which are introductory. . . . The STD RFC sub-series was created to identify those RFCs which do in fact specify Internet standards." IETF Secretariat et al., The Tao of IETF: A Guide for New Attendees of the Internet Engineering Task Force 15 (Network Working Group, Request for Comments No. 1718) (Nov. 1994), available at http://www.rfc-editor.org/rfc/rfc1718.txt. Thus, not all RFCs are Internet standards, although all Internet standards are RFCs.

18 RFC 1591, supra note 17.

19 Id.

20 Id.
Since the publication of RFC 1591, IANA has issued a number of ccTLD News Memos.\textsuperscript{21} Although many of these memos were issued for communication purposes, the first memo addressed the relationship between ccTLD managers and national governments. It stated that IANA "takes the desires of the government of the country very seriously, and will take them as a major consideration in any transition discussion."\textsuperscript{22}

Notwithstanding RFC 1591 and the first ccTLD News Memo, controversies existed. For example, RFC 1591 required that ccTLD managers reside in the requested domain. Yet, a British company successfully registered Libya's ccTLD, ".ly," by listing its owner's Tripoli address as the address of the administrative contact.\textsuperscript{23} In addition, IANA has delegated ccTLDs to unaccountable commercial entities that had limited ties to the concerned domain. Out of recourse from IANA, the government of Bhutan sought assistance from the ITU, the United Nations-affiliated body that governs international telecommunications matters, to reclaim its ccTLD, ".bt."\textsuperscript{1} Even worse, IANA was dragged into domestic disputes and had to make arbitrary decisions concerning Haiti's ccTLD ".ht,"\textsuperscript{2} which IANA eventually redelegated in January 2004.\textsuperscript{26}

\textsuperscript{21} All the ccTLD News Memos are available at http://www.iana.org/cctld/cc路虎ews.htm. The first memo appeared in October 1997. Four others were published in the next two years. The sixth memo came in October 2001, after a three-year hiatus. Released in the wake of the 2001 ICANN meeting in Los Angeles, this memo invited ccTLD managers to "initiate a bottom-up effort to assess and improve ccTLD registry security practices." Disappointedly though, the Los Angeles conference focused primarily on online security issues as a result of the September 11th terrorist attacks and sidestepped important accountability and ccTLD matters. See Verne Kopytoff, \textit{ICANN Forum Warns of Web Vulnerability}, S.F. CHRON., Nov. 17, 2001, at 1B. In February 2003, in the wake of its contract renewal with the DoC, IANA published its seventh memo, discussing Internationalized, or multilingual, domain names and its ccTLD database. IANA, ccTLD News Memo #7 (Feb. 1, 2003), available at http://www.iana.org/cctld/cc路虎ews7.htm.

\textsuperscript{22} IANA, ccTLD News Memo #1, \textit{supra} note 15.

\textsuperscript{23} MUELLER, \textit{RULING THE RoOT}, \textit{supra} note 3, at 127, 283 n.31. In June 2004, ICANN approved the partial redelegation of Libya's "".ly."" See infra note 55 and accompanying text.


\textsuperscript{26} IANA, IANA REPORT ON REDELEGATION OF THE .HT TOP-LEVEL DOMAIN (2004), available at http://www.iana.org/reports/ht-report-13jan04.htm; see also Kieren McCarthy, \textit{Haiti Kisses ICANN Ring, Rewarded with Control over Own Domain}, REGISTER, at http://
Moreover, not all political entities were included in the ISO 3166-1 list, and those omitted were understandably concerned about how IANA's actions (or the lack thereof) could frustrate their political aspirations. For example, the Palestinians did not receive the "ps" domain until the ISO 3166-1 list included the Occupied Palestinian Territory.\(^{27}\) Conversely, despite its dissolution in 1991, the Soviet Union continues to exist in cyberspace, because IANA has failed to delete the "su" domain from the root zone file.\(^{28}\) According to IANA's root-zone WHOIS information, the "su" ccTLD is currently being phased out.\(^{29}\)

The European Union is equally unhappy about the ISO 3166-1 codes. Despite its size and economic importance, it failed to obtain its "eu" name space, because the ISO 3166-1 list does not recognize supranational entities.\(^{30}\) In September 2000, the ICANN board finally passed a resolution approving the delegation of the "eu" TLD.\(^{31}\) The European Commission subsequently selected EURid as the manager of the "eu" TLD\(^{32}\) and adopted the regulation for the implementation and coordination of the "eu" name space.\(^{33}\)


\(^{28}\) See Arx & Hagen, supra note 13, ¶ 41; Sergey Kuznetsov, Russia May Say 'See Ya' to Dot-Su, WIRED NEWS, http://www.wired.com/news/print/0,1294,55687,00.html (Oct. 19, 2002).


Since the mid-1990s, the Internet has grown substantially in both size and scope; it became increasingly commercial and global. By the late 1990s, the U.S. government decided to privatize the DNS. Following a request for comments from the public, the DoC published a proposal to reform the DNS administration in January 1998. Known as the “DNS Green Paper,” this proposal mapped out the Clinton administration’s domain name policy and explained why the DoC had authority to regulate the DNS. Although the Green Paper was intended to be consultative by nature, many found the document controversial.

In light of this reaction, the DoC abandoned its original rulemaking plan. Instead, it issued a nonbinding statement of policy that became known as the “DNS White Paper.” The White Paper delineated four basic principles that were used to develop the new DNS system, namely, “stability, competition, private bottom-up coordination, and representation.” Noting the need to withdraw the U.S. government from DNS administration, the policy statement called for the establishment of a private entity that would take over the DNS. As the White Paper stated, “overall policy guidance and control of the TLDs [top-level domains] and the Internet root server system should be vested in a single organization that is representative of Internet users around the globe.”

In addition, the White Paper noted that “neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses.” Nonetheless, the

---


37 Id.

38 Id.

39 Id.
White Paper recognized the need to ensure international input into the new DNS. It also acknowledged the authority of national governments “to manage or establish policy for their own ccTLDs.”

Finally, the White Paper identified cybersquatting—the preemptive registration of trademarks as domain names by third parties—as a major problem for the DNS. It called upon WIPO to “initiate a balanced and transparent process” to provide the new entity with recommendations on how to deal with cybersquatting. Pursuant to this invitation, WIPO launched the First WIPO Internet Domain Name Process, a lengthy and extensive global consultative process that involved consultation meetings in fourteen countries in six continents and the participation of a large number of government agencies, intergovernmental organizations, professional associations, corporations, and individuals.

Shortly after the DoC published the White Paper, ICANN was incorporated as a private not-for-profit corporation in California, with Postel as its chief technical officer and a board of directors that has limited knowledge of the Internet and domain name matters. In November 1998, the DoC entered into an agreement with ICANN concerning the transfer of DNS management. To

---

40 Id.
42 Unfortunately, Postel died in October 1998, as a result of complications from open heart surgery. As Professor Mueller noted, “[h]is death robbed the organization of its moral center, a good part of its institutional memory, and most of what remained of its legitimacy.” MUELLER, RULING THE ROOT, supra note 3, at 181. For discussions and criticisms of ICANN, see generally James Boyle, A Nondelegation Doctrine for the Digital Age, 50 DUKE L.J. 5 (2000); Tamar Frankel, The Managing Lawmaker in Cyberspace: A Power Model, 27 BROOK. J. INT’L L. 859 (2002); Froomkin, Habermas@Discourse.Net, supra note 17, at 838-55; Froomkin, Wrong Turn in Cyberspace, supra note 34; A. Michael Froomkin & Mark A. Lemley, ICANN and Antitrust, 2003 U. ILL. L. REV. 1; Joseph P. Liu, Legitimacy and Authority in Internet Coordination: A Domain Name Case Study, 74 IND. L.J. 587 (1999); John Palfrey, The End of the Experiment: How ICANN’s Foray into Global Internet Democracy Failed, 17 HARV. J.L. & TECH. 409 (2004); Symposium, ICANN Governance: ICANN 2.0, 36 LOY. L.A. L. REV. 1087 (2003); Weinberg, supra note 2; Jonathan Zittrain, ICANN: Between the Public and the Private—Comments Before Congress, 14 BERKELEY TECH. L.J. 1071-93 (1999).
take over IANA's operation, ICANN also entered into an agreement with the Information Sciences Institute at the University of Southern California, where Postel worked until his untimely death.\footnote{Contract Between ICANN and the United States Government for Performance of the IANA Function, Feb. 9, 2000, \textit{available at} http://www.icann.org/general/iana-contract-09feb00.htm.}

A few months later, the DoC officially recognized ICANN as the private entity mentioned in the White Paper.\footnote{Letter from J. Beckwith Burr, Acting Associate Administrator for International Affairs, National Telecommunications and Information Administration, U.S. Department of Commerce, to David Graves, Director, Business Affairs, Network Solutions, Inc. (Feb. 26, 1999), \textit{available at} http://www.ntia.doc.gov/ntiahome/domainname/icannnewco.htm.} As Professor Michael Froomkin observed, this development was "no coincidence... 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—and could be presented as a pro-Internet, deregulatory victory for the Clinton administration (and [Presidential Senior Adviser] Ira Magaziner). ICANN exists because the Department of Commerce called for it to exist."\footnote{Froomkin, \textit{Wrong Turn in Cyberspace}, supra note 34, at 70.}

Structurally, ICANN benefits from the input of its directors, supporting organizations, and special advisory committees.\footnote{Some ICANN critics have pointed out that this formal structure existed merely on paper, not in reality. For ICANN's recent reform in December 2002, see infra text accompanying notes 62-64.} The committee that deals with global policy and ccTLD matters is the Governmental Advisory Committee ("GAC"), which is regularly attended by national governments, distinct economies, and intergovernmental organizations, such as the ITU and WIPO. Under the recently reformed structure, the GAC provides direct advice to the ICANN board and appoints liaisons to the board, the committee that nominates the directors, and the various supporting organizations.\footnote{ICANN, \textit{ICANN AND THE GLOBAL INTERNET} 4 (2003), \textit{available at} http://www.itu.int/itucdoc/itu-t/workshop/cctld/024r1.html. See generally Wolfgang Kleinwaechter, \textit{From Self-governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources}, 36 \textit{LOY. L.A. L. REV.} 1103, 1115-18 (2003), for discussion of the GAC.}

To "announce" its taking over of IANA's function and to emphasize its authority over ccTLD matters, ICANN issued ICP-1 in May 1999.\footnote{IANA, ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation) (May 1999), \textit{available at} http://www.icann.org/icp/icp-1.htm} Combining RFC 1591 and the ccTLD News Memo #1,
this document strengthened the power of national governments on ccTLD matters. As it stated, "[t]he desires of the government of a country with regard to delegation of a ccTLD are taken very seriously. The IANA will make them a major consideration in any TLD delegation/transfer discussions."\(^5\)

In February 2000, the GAC presented to ICANN the Principles for Delegation and Administration of ccTLDs ("GAC Principles"),\(^5\) which ICANN later used extensively to justify their redelegation efforts. Although the GAC Principles sought to provide "the model for institutionalizing the relationship between ICANN, ccTLD delegations, and the relevant national governments or public authorities,"\(^5\) many found the document controversial and antithetical to the interests of ccTLD managers.

Since its establishment, ICANN, acting as IANA, has delegated the ".ps" domain to the Occupied Palestinian Territory, deleted Zaire's ".zr" in response to the country's change of name,\(^5\) and redelegated more than a dozen other ccTLDs, including Canada's ".ca," Australia's "au," and Japan's "jp."\(^5\) ICANN also approved the partial redelegation of Libya's ".ly," whose name

---

50 ICP-1, supra note 49.
52 MUELLER, RULING THE ROOT, supra note 3, at 206. As the GAC Principles noted:
    The relevant government or public authority ultimately represents the interests of the people of the country or territory for which the ccTLD has been delegated. Accordingly, the role of the relevant government or public authority is to ensure that the ccTLD is being administered in the public interest, whilst taking into consideration issues of public policy and relevant law and regulation.
    GAC Principles, supra note 51, § 5.1.
server ceased functioning in April 2004, and is working on the redelegation of Iraq’s “.iq” as of this writing. With the exception of Canada, ICANN has entered into contractual relationships with all of the new ccTLD managers upon full redelegation. Virtually all of these redelegation efforts seem uncontroversial, as they require only one report; only Australia and Japan require two reports.

In addition, ICANN has been working actively with other ccTLD managers to document their relationships. These relationships vary greatly with respect to the type of organization, management policies, economics, language, culture, legal environment, and relations with governments. While ICANN expected ccTLD managers to enter into contracts in which they would acknowledge ICANN’s authority and would agree to contribute fees to the organization, the managers refused. Instead, the managers questioned ICANN’s authority and criticized the organization for its lack of openness, accountability, and representation.

In February 2002, then-ICANN President Stuart Lynn openly admitted the need for reforms, which critics had advocated since ICANN’s establishment. He wrote, “if ICANN comes to be seen


57 See McCarthy, Haiti Kisses ICANN Ring, supra note 26 (criticizing ICANN’s redelegation process). Notably, ICANN did not enter into an agreement with Neustar, the “.us” ccTLD manager. See Arx & Hagen, supra note 13, ¶ 37.


60 See Model ccTLD Sponsorship Agreement—Triangular Situation (Initial Version), Sept. 2, 2001, available at http://www.icann.org/cclds/model-tscsa-02sep01.htm; see also Arx & Hagen, supra note 13, ¶¶ 32-34 (discussing ICANN’s contractual powers).

as simply a tool of the U.S. Government, it will no longer have any hope of accomplishing its original mission."\(^{62}\) Seeking to reconcile the organization’s relationship with ccTLD managers, the proposal recommended that ICANN replace the five at-large board seats with government representatives.

In December 2002, ICANN finally completed its reforms, beginning what some commentators have called "ICANN 2.0."\(^{63}\) Under the new structure, ICANN has a volunteer board of directors, including fifteen voting members and six non-voting liaisons, all of whom are to be selected by ICANN’s Nominating Committee, supporting organizations, and special advisory committees.\(^{64}\)

To facilitate the interests of ccTLD managers and national governments, a new Country Code Domain Name Supporting Organization ("ccNSO") was established.\(^{65}\) Under this new structure, ccTLD managers dissatisfied with ICANN’s policies can appeal to the ccNSO to determine whether the consensus policies apply to

\(^{62}\) Id.


\(^{64}\) The fifteen directors include the President, eight voting members selected by the Nominating Committee, and two each by the Address Supporting Organization ("ASO"), the Country Code Names Supporting Organization ("ccNSO"), and the Generic Names Supporting Organization ("GNSO"). Bylaws for Internet Corporation for Assigned Names and Numbers, as amended Oct. 13, 2003, art. VI, § 2(1) [hereinafter ICANN Bylaws], available at http://www.icann.org/general/archive-bylaws/bylaws-13oct03.htm. The six non-voting liaisons are appointed, respectively, by the Governmental Advisory Committee ("GAC"), the Root Server System Advisory Committee ("RSSAC"), the Security and Stability Advisory Committee ("SSAC" or "SECSAC"), the Technical Liaison Group ("TLG"), the At-Large Advisory Committee ("ALAC"), and the Internet Engineering Task Force ("IETF"). Id. § 9(1).

\(^{65}\) The ccNSO was established upon the enrollment of thirty ccTLD managers with at least four within each geographic region as stated in ICANN’s Bylaws. See Formation of the Country-Code Names Supporting Organization (ccNSO), at http://ccnso.icann.org/announcements/ccnso-statement-01mar04.pdf (Mar. 1, 2004). The ccNSO was charged with the responsibility "for developing and recommending to the Board global policies relating to country-code top-level domains, nurturing consensus across the ccNSO’s community, including the name-related activities of ccTLDs, and coordinating with other ICANN Supporting Organizations, committees, and constituencies under ICANN." Web site of the Country Code Names Supporting Organization, at http://ccnso.icann.org/ (last visited July 23, 2004).
the concerned ccTLDs. After all, "ICANN was not designed at its creation to have direct oversight of ccTLD policy." By adding this structure, ICANN seeks to protect itself from sensitive national sovereignty issues.

While ICANN remains relevant to the ccTLD debate, the increasing concern of ccTLD managers and national governments over ccTLD policymaking might affect how ICANN develops its policy. As Kenneth Cukier pointed out, ccTLD managers have the potential to control ICANN's future: "The confederation of independent ccTLD administrators could bring ICANN vitally-needed legitimacy and funding if it formally recognizes the authority of ICANN and pay it [sic] fees. Conversely, if the ccTLD community continues to balk from establishing a formal relationship with ICANN, it would weaken the institution." In fact, if the ccTLD managers can convince the DoC that ICANN cannot handle ccTLD matters, the DoC might decide not to renew ICANN's contract.

---

66 ICANN Bylaws, supra note 64, art. IX, § 4(11). Article IX of ICANN's Bylaws provides, in relevant part:

[Any ccTLD manager who becomes a ccNSO member] may provide a declaration to the ccNSO Council stating that (a) implementation of the policy would require the member to breach custom, religion, or public policy (not embodied in the applicable law described in paragraph 10 of this Section), and (b) failure to implement the policy would not impair DNS operations or interoperability, giving detailed reasons supporting its statements. After investigation, the ccNSO Council will provide a response to the ccNSO member's declaration. If there is a ccNSO Council consensus disagreeing with the declaration, which may be demonstrated by a vote of 14 or more members of the ccNSO Council, the response shall state the ccNSO Council's disagreement with the declaration and the reasons for disagreement. Otherwise, the response shall state the ccNSO Council's agreement with the declaration. If the ccNSO Council disagrees, the ccNSO Council shall review the situation after a six-month period. At the end of that period, the ccNSO Council shall make findings as to (a) whether the ccNSO members' implementation of the policy would require the member to breach custom, religion, or public policy (not embodied in the applicable law described in paragraph 10 of this Section) and (b) whether failure to implement the policy would impair DNS operations or interoperability. In making any findings disagreeing with the declaration, the ccNSO Council shall proceed by consensus, which may be demonstrated by a vote of 14 or more members of the ccNSO Council.

Id.


68 CUKIER, supra note 24, at 2.

69 Most recently, the DoC and ICANN agreed to extend their joint MOU for three additional years until September 30, 2006. Press Release, ICANN and U.S. Department of
Apart from ccTLD managers, national governments have played an increasingly important role in the ccTLD debate. In a recent survey, Professor Michael Geist found a diverse array of relationships between national governments and ccTLD managers. While government agencies and departments manage ten ccTLDs, national governments have contractual or informal relationships with many others. Some registries, like those in Canada and the United States, also create a relationship between the country and the domain name registrants by requiring local presence as a prerequisite to registration.

Today, national governments recognize ccTLDs "as a component of their sovereignty and a vital national interest." Realizing that ccTLDs may denote the "brand of the country," some governments openly embrace ccTLDs as "a platform for national economic growth and the institutions of civil society brought online." Some, like Tuvalu, even use ccTLDs as a revenue-generating

---


71 As Professor Geist stated:

Forty-seven percent [of the fifty-six countries that responded to the survey] indicated that they retain ultimate control in one of four ways. First, many governments directly operate the national ccTLD as part of a government ministry or agency. Second, some governments have established a subsidiary company of a government ministry or agency to manage their ccTLD. Third, several governments have enacted legislation granting themselves final authority over their ccTLD's operations. Fourth, a number of governments have entered into operational contracts with their national ccTLD manager in which they assert their ultimate authority over the ccTLD, but grant their approval to a non-governmental ccTLD manager.


72 Arx & Hagen, supra note 13, ¶ 21.

73 CUKIER, supra note 24, at 1. As Professor Mueller explained:

Just as the physical world was divided up into mutually exclusive territories controlled by sovereign governments, so could the name space be. Country codes were the most direct and obvious point of entry for this kind of thinking. If national governments could gain control over the assignment of their own country code, they could translate their geographic jurisdictions into cyberspace and gain a significant role for themselves in Internet governance.

MUELLER, RULING THE ROOT, supra note 3, at 205.

74 CUKIER, supra note 24, at 1.
source, selling off rights in its name space for tens of millions of dollars.\textsuperscript{75}

As ccTLDs become increasingly important, national governments begin to assert control over the administration of their ccTLDs. For example, Australia, Canada, and Japan have petitioned ICANN for the redelegation of their domains. Likewise, the European Union is working closely with ICANN to create the ".eu" name space.\textsuperscript{76}

Not all governments, however, are interested in working with ICANN. Some prefer to act alone, or to abandon ICANN for a more favorable international forum, such as the ITU.\textsuperscript{77} Indeed, some governments have already sought to use national legislation to regulate local ccTLD managers. The government of South Africa, for instance, recently introduced legislation to reclaim control of the ".za" name space from the incumbent ccTLD manager.\textsuperscript{78} Similarly, during the controversial redelegation of the ".au" domain, the Australian government reminded ICANN that "as a last resort the Australian Government could invoke legislation relating to the self-regulation of the domain name system."\textsuperscript{79}

Legally, some governments can consider using the "eminent domain" doctrine (or its equivalent),\textsuperscript{80} which, if applicable, allows governments to take away private property at fair market value to promote an overriding public interest.\textsuperscript{81} Given the socio-economic importance of a ccTLD, these governments are likely to be able to convince the courts that their actions are constitutional. Nonetheless, such governmental action might be undesirable, as it would

\textsuperscript{75} Kate Mackenzie, \textit{Tuvalu's .tv Yields $88m}, \textit{Australian}, Jan. 29, 2002, at 27.


\textsuperscript{78} In March 2002, the government of South Africa introduced the Electronic Communications and Transactions Bill, which proposed to set up a new domain name authority within South Africa with board members chosen by the Minister of Communications. See Arx & Hagen, \textit{supra} note 13, ¶ 23; Geist, \textit{ccTLD Governance Project}, \textit{supra} note 70.

\textsuperscript{79} Letter from Richard Alston, Senator and Minister for Communications, Information Technology and the Arts, Australia, to M. Stuart Lynn, President and CEO, ICANN (July 4, 2001), available at http://www.iana.org/cctld/au/alston-to-lynn-04jul01.htm.

\textsuperscript{80} Cukier, \textit{supra} note 24, at 6; see also id. (outlining a plan to nationalize ccTLDs).

\textsuperscript{81} See generally Roter A. Cunningham et al., \textit{The Law of Real Property} 505-12 (2d. ed., 1993); Nichols on Eminent Domain (Perm. ed., 2003).
bring formal political control over the ccTLD system and impose constraints on the DNS that ICANN was designed to prevent.\textsuperscript{82}

To break free of ICANN, governments can join together to establish an alternative root zone file, or a system of root zone files, that replaces the current root zone file. ICANN's governance structure is premised on the general consensus that there can be only one authoritative root zone file, lest there be inefficiency, in-connectivity, economic injury, or even chaos in the DNS. However, if governments become so frustrated with ICANN that they would rather risk infrastructure damages than remain subjected to an overbearing "Leviathan," many might consider alternative root zone files desirable.\textsuperscript{83}

Finally, in the absence of ICANN's intervention or oversight, the international community can work together to develop a "code of practice" to promote harmonization and compliance while minimizing disputes. For example, they can draft an international treaty that sets the parameters of ccTLD management and administration practice. They also can work together to develop a non-binding document that provides guiding principles to ccTLD managers and national governments.

A case in point is the WIPO ccTLD Best Practices for the Prevention and Resolution of Property Disputes,\textsuperscript{84} which WIPO released in June 2001. This document provides voluntary guidelines concerning registration practices and dispute resolution procedures. These guidelines were particularly needed, because ccTLD managers retain the power to set policies for their domain. For example, they can decide whether registrants have to be residents of the country, whether they are subject to the Uniform Dispute Resolution Policy ("UDRP"), and whether their personal information will be displayed on a publicly available WHOIS database.

\begin{footnotes}
\item[82] Cukier, supra note 24, at 6.
\item[83] See Arx & Hagen, supra note 13, ¶ 83 (advocating the acknowledgment by national governments that each nation is authoritative for its respective ccTLD and the introduction of a peer-to-peer protocol into the DNS). Theoretically, any computer can resolve domain names by querying different name servers that point to different root servers. Alternative top-level domains and alternative root servers indeed exist. Nonetheless, very few computers look up domain names using alternative root servers, and the vast majority rely on the set of thirteen "legacy" root servers to resolve domain names. See Mueller, Ruling the Root, supra note 3, at 53-55; Weinberg, supra note 2, at 197-98.
\end{footnotes}
Of notable interest is the final section of this document, which advocates the adoption of the UDRP in the absence of any contrary local privacy regulations.\(^8\) Introduced in October 1999, the UDRP set forth the terms and conditions related to a dispute between the registrant and a third party over the registration and use of a domain name.\(^6\) Although commentators have criticized the UDRP for its procedural weaknesses,\(^8\) the policy has been widely acclaimed for its simplicity and cost-effectiveness in resolving trademark disputes. Since the UDRP entered into force in December 1999, thousands of cases have been filed, and the majority of these cases has been resolved satisfactorily and efficiently.

In recent years, the ITU, like WIPO, has begun to play a much larger role in the ccTLD debate. In December 2003, the ITU conducted the first phase of the World Summit on the Information Society ("WSIS") in Geneva, bringing together national leaders, government officials, corporate executives, industry experts, and representatives of nongovernmental organizations and civil society. At this summit, government leaders from less developed countries and representatives of civil society expressed great concern over ICANN's illegitimate and arbitrary role in Internet governance, its close ties to the U.S. government, and its failure to take account of interests of other nations.

85 The Uniform Domain Name Dispute Resolution Policy is available at http://www.icann.org/dndr/udrp/policy.htm (last updated May 17, 2002).

86 Under the UDRP, each registrant agrees to participate in a mandatory administrative proceeding when a third party complains to a dispute resolution service provider. The person bringing the case must then prove not only that the registrant's domain name is identical, or confusingly similar to a trademark, or service mark, in which the complainant has rights, but also that the person who registered the domain has no rights to, or legitimate interests in, the domain name and the domain name has been registered and is being used in bad faith.

87 Among the criticisms are the selection and composition of the dispute resolution panel, the failure to provide adequate time for a domain name registrant to reply to a complaint, the failure to ensure that the registrant has received actual notice of the complaint, and the registrant's limited access to courts for review when the dispute resolution panel decides against a party. For criticisms of the UDRP, see generally Michael Geist, Fair Com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP, 27 BROOK. J. INT'L L. 903 (2002); A. Michael Froomkin, ICANN's "Uniform Dispute Resolution Policy"—Causes and (Partial) Cures, 67 BROOK. L. REV. 605 (2002). See also Laurence R. Helfer & Graeme B. Dinwoodie, Designing Non-national Systems: The Case of the Uniform Domain Name Dispute Resolution Policy, 43 WM. & MARY L. REV. 141 (2001); Froomkin, Wrong Turn in Cyberspace, supra note 34; MILTON MUELLER, ROUGH JUSTICE: AN ANALYSIS OF ICANN'S UNIFORM DISPUTE RESOLUTION POLICY (2003), available at http://www.acm.org/usacm/IG/roughjustice.pdf.
Interestingly, ICANN and the DNS represent only a small portion of the Internet governance issue, and even a smaller portion of the information society debate. Other issues include privacy, spam, online pornography, hate speech, cybersecurity, identity theft, cyberstalking, and intellectual property rights. Nevertheless, ICANN has attracted major attention from the delegates. At the end of the summit, the delegates were unable to reach a consensus. Instead, they called upon United Nations Secretary-General Kofi Anan to create a special working group on Internet governance. As the WSIS Declaration of Principles, one of the summit’s two key documents, stated:

International Internet governance issues should be addressed in a coordinated manner. We ask the Secretary-General of the United Nations to set up a working group on Internet governance, in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organizations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005.88

Once established, this working group will study the Internet governance issue; consult with experts from governments, the private sector, and civil society; and provide policy recommendations, if applicable, in the summit’s second phase in Tunis in November 2005. By setting up this working group, the international commu-

88 WSIS Declaration of Principles ¶ 50 (Dec. 12, 2003), available at http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf; see also David McGuire, *U.N. Sets Aside Debate over Control of Internet*, WASH. POST, Dec. 9, 2003, at E5. According to the complementary WSIS Plan of Action, this working group should, inter alia:

i) develop a working definition of Internet governance;

ii) identify the public policy issues that are relevant to Internet governance;

iii) develop a common understanding of the respective roles and responsibilities of governments, existing intergovernmental and international organisations and other forums as well as the private sector and civil society from both developing and developed countries;

iv) prepare a report on the results of this activity to be presented for consideration and appropriate action for the second phase of WSIS in Tunis in 2005.

nity successfully rejuvenated the participation of intergovernmental organizations in the ccTLD debate.

Immediately after the summit, various intergovernmental organizations began to jockey for political positions in anticipation of the establishment of the U.N. working group. For example, in February 2004, the ITU conducted a Workshop on Internet Governance, which sought to “provide a forum for invited experts to exchange views and make analytical studies on definitions, viewpoints and visions on Internet governance from several aspects, including legal, technological, administration and commercial issues.” A month later, the United Nations Information and Communication Technologies Task Force conducted its Global Forum on Internet governance in New York, with the stated goal of providing “an opportunity for all relevant stakeholders—including those who are not members of the Task Force—to engage in an open discussion of all aspects of Internet governance.”

Most recently, ICANN and the ITU jointly sponsored a workshop on ccTLDs, which immediately followed the ICANN’s meeting in Kuala Lumpur. As stated on its Web site, this open workshop was conducted “to focus on the operation and practical operational issues facing the ccTLDs and to give the opportunity for ccTLD operators and ITU Member States to share their experiences.” While the cooperation between ICANN and the ITU represents a promising development, this arrangement strongly suggests the highly sensitive nature of ccTLD governance after WSIS.

Over the next few years, the struggle for control of the DNS and ccTLD delegations is likely to continue, or perhaps even escalate. There is little doubt that the ccTLD policymaking story will still include ICANN, IANA, ccTLD managers, national governments, GAC, ITU, and WIPO. The story will also feature new, emerging players, such as CCNSO, CENTR (Council of European

---


National Top-Level Domain Registries),\textsuperscript{92} powerful individual ccTLD managers,\textsuperscript{93} intellectual property rights holders, Internet service providers, and major telecommunications and information technology companies. As a result, few can forecast how the future will unfold, and it can only become more intriguing.

To help us better understand ICANN, the international domain name system, the ccTLD debate, and quasi-governmental lawmaking processes, the Cardozo Intellectual Property Law Program and the Cardozo Journal of International & Comparative Law co-sponsored the "ICANN, ccTLD, and the Legacy Root: Domain Name Lawmaking and Governance in the New Millennium" Symposium on March 17, 2003. This event brought together academics, legal practitioners, government officials, and representatives of intergovernmental and nongovernmental organizations. What follows are some of the papers presented at this Symposium. I hope you will enjoy them.

\textsuperscript{92} CENTR is an international association of ccTLD registries. CENTR provides a forum to discuss policy matters concerning ccTLD registries, acts as a channel of communication to Internet governing bodies and related organizations, and promotes the interests of not-for-profit ccTLDs by lobbying on their behalves. Although CENTR has a European focus, full membership is open to all ccTLD registries. Among the non-European members are CIRA (for Canada), IPM (for Iran), ISOC-IL (for Israel), and the Palestinian Registry. The CENTR's Web site is available at http://www.centr.org.

\textsuperscript{93} Examples of these powerful ccTLD managers include Nominet UK (".uk") and DENIC (".de"), each of which has millions of registrations. See Michael Geist, \textit{Governments Hold Reins in Those National Domains}, \textit{Toronto Star}, Mar. 10, 2003, at 3D.