International and National Regulation of the Internet

A. Michael Froomkin
University of Miami School of Law
froomkin@law.miami.edu
Submitted Dec. 8, 2003

Although the title for this paper set by the organizers of this Round Table discussion is "the international and national regulation of the Internet," the instructions which accompanied this title explained the topic as "the governance issues regarding ICANN" and "similar issues existing with the national registry activities". The tension between the broad title and substantially narrower-seeming subtitle reflects something real about the contemporary nature of regulation of the Internet and its infrastructure.

I. Introduction: Three Spheres of Internet Regulation

Broadly speaking, Internet regulation today can be conceived of as involving three related spheres: Direct regulation of the internet infrastructure itself; regulation of activities that can be conducted only over the internet; and, regulation of activities which can be, but need not be, conducted over the Internet.

The first sphere: Direct regulation of the internet infrastructure itself, including
a. the standards of communication,
b. the equipment used to provide and access Internet communication,
c. intermediaries engaged in the provision of Internet communications, e.g. Internet Service Providers (ISPs)

The second sphere: Regulation of activities that can be conducted only over the internet and which have no significant off-line analogues. An example is the regulation of anonymous online communication via anonymizing re-mailers.

The third sphere:. Finally, there is the regulation of the enormous category of activities which may or may not be conducted over the internet, e.g. e-commerce in both tangible and intangible goods. In many cases the Internet version of an activity often will simply be swept up in the general regulation of the type of conduct.

(a) In some cases, however, the Internet version may be subject to special or additional regulation because the use of the Internet is seen as somehow aggravating an underlying problem or offense. An example of this is US attempts to regulate the provision of obscene or "indecent" content to minors via the Internet.

(b) In other cases, there may be attempts to craft special regulations for the Internet version of an activity because of fears that its international character (and concomitant regulatory arbitrage), the ease of anonymization, or the elimination of formerly prohibitive transactions costs changes the danger, incidence, or character of the activity -- or, most commonly, makes the enforcement of the pre-existing rules difficult or impossible. Examples of this include attempts

to regulate peer-to-peer sharing of material copyrighted by others and regulation (or in some cases discouragement) of e-cash.

These spheres of regulation are obviously related in many ways. What matters most for current purposes, however, is that this schema underlines why approaches to the first sphere of regulation, direct regulation of the infrastructure, have two sometimes radically different sets of motives even though the regulatory techniques and tools often may overlap or even interfere with one another.

On the one hand, some regulatory (or de-regulatory) strategies pursue goals that are primarily internal to the first sphere. For example, as described below, the current Internet architecture depends on the unique assignment of Internet Protocol numbers; the regulation of the mechanisms that control assignment of these potentially valuable resources -- and which determine when and how the underlying standards might be modified -- is a matter of critical importance to the Internet, one that is (currently) internal to the first sphere.[1] Similarly, the regulation of the creation of new Top-Level Domains (TLDs) and the regulation of the assignment of Second-Level Domains (SLDs) are in the first instance an issue in the first sphere, albeit one influenced by external rules such as trademark law.[2]

More generally, a number of independent, private, non-profit, standards bodies define the technical standards for various parts of the Internet. These groups include the Internet Engineering Task Force (IETF), an unincorporated international volunteer organization of software and network engineers, and the W3C, a consortium of corporations and interested individuals who concentrate on HTML and WWW-oriented standards. These bodies do not, however, tend to venture beyond classic standard-setting activities.

In contrast, other bodies, notably governments and industry pressure groups, seek to facilitate and deploy regulatory strategies that regulate the Internet infrastructure. Their goal is to leverage control over that infrastructure to achieve social goals external to the infrastructure itself. An example of this are calls to expand the information that domain name registrants must publish in the WHOIS database in order, for example, to allow copyright owners to know to what address they should address their writs in the event that they believe that their rights are being infringed online.

The contrast between what I have labeled the internal and external motivations not only influences the type of rule likely to be advanced, but more importantly has institutional implications. Of these, the most critical is the type of regulatory body likely to be seen as a legitimate source of the rule in question. Questions about the mis-match between legitimacy and effectiveness lie at the heart of both current and future debates about the regulation of the

[1]Possible external constraints, such as competition law concerns, have not to date materialized.

[2]As we shall see below, however, even here assignment rules can be determined by external social policies.

Internet infrastructure. Many bodies -- governments -- with legitimacy to make rules in the second and third spheres lack, or believe they lack, the ability to regulate the infrastructure effectively; the most apparently effective bodies extant today, the Internet Corporation for Assigned Names and Numbers (ICANN) and its seemingly subsidiary body, the Internet Assigned Numbers Authority (IANA) face substantial questions about their legitimacy, especially when they venture out of the first sphere. There is more acceptance of the legitimacy of established technical standard setting bodies such as the IETF and the W3C but this is in large part because they tend to restrict their activities firmly to the first sphere, and also because there is greater respect for the quality of their decisions (or, perhaps, less general knowledge of them). In contrast, ICANN already acts like a market regulator, and faces pressures to expand its remit further into realms ordinarily occupied by governments. Simultaneously, governments are taking an increasingly direct role in this supposedly private body's decision-making via the "Government Advisory Committee" (GAC), but are doing so in a manner notably lacking in transparency.

Dissatisfaction with ICANN, and the US government's, role as the most powerful and only truly global regulator in the first sphere has led to many calls for a new system of regulation. One approach has been to try to reform ICANN, although it is unlikely that the most recent set of 'reforms' successfully addresses the legitimacy problem. Another approach has been to find alternate institutions that might take on the jobs ICANN handles, and perhaps others more global Internet regulation also. One self-nominated candidate is the ITU, which is currently sponsoring the World Summit on the Information Society. A third approach uses the traditional apparatus of bilateral and multilateral treaties to address particular issues arising from the Internet that are thought to require trans-national regulation.[3]

II. Technical Interlude

To best appreciate the governance issues, it is useful to have an understanding of the relationship between internet IP numbers and domain names, and also of the parties involved in the assignment of these critical internet identifiers. Technically expert readers can skip to Part III below.

A. IP Numbers

Internet Protocol numbers (IP numbers) provide the identifying information that allows an e-mail to find its destination or allows a request for a web page to reach the right computer across the Internet. The Internet as we know it could function without domain names. It could function, albeit differently, with radically different systems for allocating domain names. The Internet as we know it cannot function without a system for the unique allocation of Internet Protocol numbers. Control over this resource may be the most critical choke point in Internet regulation, albeit one that has not as yet been exploited in any manner.

The majority of the Internet relies on the IPv4 system, four numbers of up to three digits separated by dots. Due to a perceived shortage of 32-bit IPv4 numbers, the IETF proposed the

[3]In some cases, alas, part of the motivation for the treaty approach may be to insulate policy decisions from national legislatures.

replacement with a new standard, IPv6, which uses 128-bit addresses; other bodies such as ICANN have endorsed this change. Assignment of both sets of IP numbers is primarily in the hands of IANA and the Regional Internet Registries, although ICANN also plays a small role. Three of the five RIRs pre-date ICANN and have carried on their functions without substantial change since ICANN's creation, other than the hiving-off of part of their geographical coverage.[4] In June 2001, ICANN adopted a proposal from the then-existing RIRs[5] setting up "Criteria for the Establishment of New Regional Internet Registries."[6] Applying these criteria, ICANN approved the creation of AfriNIC, a new RIRs for Africa[7] and LACNIC, a new RIR for South America and the Carribean.

As a formal matter, RIRs receive delegations of unused IP address blocks from IANA,[8] although in practice the method of delegation is one determined by the RIRs themselves. The RIRs then sub-delegate smaller address blocks to various classes of users and other intermediaries (including ISPs).[9]

B. Domain Names and TLDs

Domain names are a method of defining user-friendly identifiers for internet resources which map to IP numbers. Numbers, especially long ones, are hard to remember; names are easier. Using numbers as stable front-end identifiers mapped to less-visible IP numbers also allows the owners of resources, such as web pages, to relocate them to new hardware (with a new IP number) seamlessly from the viewpoint of readers and customers.

---

[4] *See ASO Memorandum of Understanding, at* http://www.aso.icann.org/docs/aso-mou.html.

[5]The Asia Pacific Network Information Centre (APNIC), which serves the Asia/Pacific region; American Registry for Internet Numbers (ARIN), which then served the Americas and sub-Saharan Africa; and RIPE Network Coordination Centre (RIPE NCC), which served Europe and surrounding areas.

[6] *See ICANN Stockholm Meeting Topic: Criteria for Establishment of New Regional Internet Registries, at* http://www.icaan.org/stockholm/emerging-rir-topic.htm (last modified May 24, 2001).

[7]See http://www.afrinic.org/

[8]While previously an independent body, and still the subject of an independent contractual agreement between ICANN and the U.S. Department of commerce, IANA is currently run as little more than a subsidiary of ICANN. However, ICANN takes the view that it is not required to use the same public procedures in making IANA decisions that it applies to ICANN decisions. Instead "IANA" uses methods based on the practices used by Jon Postel prior to the formation of ICANN.

[9] *See, e.g.,* AKIHIRO INOMATA ET AL., IPV6 ADDRESS ALLOCATION AND ASSIGNMENT POLICY (Takashi Arano et al. eds., 2003), *at* http://www.ripe.net/ripe/docs/ipv6policy.html

There are many "top level domain names" (TLDs), including .com and also 244 "country-code top-level domains" (ccTLDs), all of which are two-letter codes, and most of which use the two letters associated by ISO Standard 3166 to refer to a country. Thus, Canada's ccTLD is .ca, and Columbia's is .co. These ccTLDs are managed either by national governments, or by private citizens domiciled in the relevant nation, ensuring that the government has regulatory authority over the ccTLD. Until recently, all TLDs and indeed all domain names, had to be expressed in a low-ASCII subset of the Latin alpha-numeric characters, but the IETF has defined[10] an encoding mechanism that will allow the simulation[11] of other character sets. There are currently no internationalized TLDs, but there are now internationalized SLDs. In March 2003, ICANN set up a mechanism by which the registrars subject to its authority would be allowed to begin registering IDNs.[12]

The current domain name system requires that each domain name be "unique" in the sense that it be managed by a single registrant rather than in the sense that it be associated with a single IP number. The registrant may associate the domain name with varying IP numbers if that will produce a desired result. For example, a busy website might have several servers, each with its own IP number, that take turns serving requests directed to a single domain name.

Traditionally, second level domain names, such as "example" in example.ca, have been allocated on a first come, first serve basis. Every ccTLD has its own rules; some impose limits on who can register what, but others do not. This sometimes results in unhappy trademark and service mark owners, late to the Internet, discovering that "their" name is already registered by another. In some cases the earlier user is a legitimate business from a different sector, or is a non-commercial user who cannot be considered an infringer. But in other cases, the first registrant is either a standard trademark infringer, or a so-called "cybersquatter" -- a person who in the business of registering domain names in the hope of reselling them to owners of identical marks, and who counts on the high cost of litigation, or its slow pace, to negotiate a windfall.

The name resolution side of the domain name system is an interdependent, distributed, hierarchical database. At the top of the hierarchy lies a single data file that contains the list of the

---

[10]String Preparation (stringprep), RFC 3454 (published December 2002); IDNs in Applications (IDNA), RFC 3490 (published March 2003); Name Preparation (nameprep), RFC 3492 (published March 2003); Encoding Scheme (punycode), RFC 3491 (published March 2003

[11]Properly configured software will show the user Kanji and other non-ASCII characters, but the underlying internet architecture will not change. The software will transform the non-ASCII characters into the ASCII required by the DNS which will not itself change. *See Naming and Directory Services: IDN Standards, at* http://www.verisign.com/nds/naming/idn/learn/standards.html for an explanation.

[12] *See ICANN Rio de Janeiro Meeting Topic: Internationalized Domain Names, at* http://www.icaan.org/riodejaneiro/idn-topic.htm (last modified Mar. 13, 2003); *Internationalized Domain Names, at* http://alac.icann.org/idn/ (last modified Apr. 7, 2003).

machines that have the master lists of registrations in each TLD. This is the "root zone," or "root," also sometimes known as the "legacy root."[13]

Domain names are resolved to IP numbers by sending queries to a set of databases linked hierarchically. The query starts at the bottom, at the name server selected by the user or her ISP. A name server is a network service that enables clients to name resources or objects and share this information with other objects in the network. If the data is not in the name server, the query works its way up the chain until it can be resolved. At the top of the chain is the root zone file maintained in parallel on thirteen different computers (the "root servers"). These thirteen machines, currently identified by letters from A-M, contain a copy of the list of the TLD servers that have the full databases of registered names and their associated IP numbers. (To confuse matters, some of these machines have both a copy of the root zone file and second-level domain registration data for one or more TLDs.[14]) Each TLD has a registry that has the authoritative master copy of the second-level domain names registered for that TLD, and the root zone file tells domain name resolving programs where to find them.

There may be a limit to the number of TLDs that can safely be inserted into the legacy root zone file, but even the most conservative estimates currently suggest that this number is well in excess of 1,000, probably 10,000 TLDs, and some technical experts suggest the true number is orders of magnitude higher. Whoever controls the root zone file determines which TLDs are visible to almost all Internet users, and also can control who will enjoy the potentially valuable franchise of running the registry for that TLD.

C. Registrars, Registries

For each TLD, a *registry* controls the database that records the authoritative controller[15] for each delegated second-level domain name.[16] *Registrars* are the bodies that interface with

[13]Although there is no technical obstacle to anyone maintaining a TLD that is not listed in the legacy root, these "alternate" TLDs can only be resolved by users whose machines, or Internet service providers (ISPs) as the case may be, use a domain name server that includes this additional data or knows where to find it. A combination of consensus, lack of knowledge, and inertia among the people running the machines that administer domain name lookups means that domain names in TLDs outside the legacy root, e.g., http://lightning.faq, cannot be accessed by the large majority of people who use the Internet, unless they do some tinkering with obscure parts of their browser settings.

[14]To further confuse matters, the "F" server is itself distributed and parallelized via Anycast.

[15]I use the word "controller" to avoid the controversial question of the nature of the registrant's legal interest in a domain name. Some argue it is a property interest, others an intellectual property interest, still others a *sui generis* intellectual property-like interests. Registries usually contend the registrant has only a contractual interest created by a service contract for term.

registrants to collect the necessary information to effectuate the delegation of a domain name, often for a fee. In order to achieve this the registrar must first query the registry to see if the SLD is available, then cause the registration information to be recorded in the registry so that future queries will note it as taken.

The registration side of the current DNS architecture is arranged hierarchically to ensure that each domain name is unique. In theory (ignoring software glitches and certain complexities introduced by the "shared registry" concept) having a single registry ensures that once a name is allocated to one person, it cannot simultaneously be assigned to a different person. End-users seeking to obtain a unique domain name must obtain one from a registrar. A registrar can be the registry or it can be a separate entity that has an agreement with the registry for the TLD in which the domain name will appear. Before issuing a registration, the registrar queries the registry's database to make certain the name is available. If it is, it marks it as taken, and (currently) associates various contact details provided by the registrant with the record.

In some TLDs, notably smaller ccTLDs, the registrar and the registry are the same body, but in .com and the other large TLDs there are many registrars authorized to sell registrations in the registry. There must be one master registry per TLD, however, in order to guarantee the uniqueness of the registrations.

III. ICANN's Functions and Its Legitimacy Deficit

The locus of ultimate control over the Internet's naming infrastructure can be debated. In one view, the real control belongs to the thirteen root servers. For if they were collectively and unanimously to decide to ignore the legacy zone file and instead take this small file from another source, that other source would become able to create (or destroy) TLDs at will. For reasons beyond the scope of this paper, however, such cooperation among the thirteen root servers is unlikely absent an almost unimaginatively radical disruptive act by the managers of the legacy root.[17]

Even more plausibly one could argue that the RIRs really control the numbering system, and that ICANN's role is primarily that of a shield against any possible competition law concerns. There is little question that at present the RIRs substantially call the tune in their relation with ICANN. ICANN proposed to the RIRs that they enter into contracts with it. Indeed, ICANN's MOU with the US government requires agreements with the RIRs as a

---

[16]The controller of the second level domain name can decide whether and how any third- and Nth-level domain names under that SLD might be sub-delegated.

[17]For the argument *see* A. Michael Froomkin, *Form and Substance in Cyberspace*, 6 J. SMALL & EMERGING BUS. L. 93 (2002), *available at* http://personal.law.miami.edu/~froomkin/articles/formandsubstance.pdf. I have speculated elsewhere that an attempt to de-list a country from the root for political reasons might be sufficiently catastrophic, but as a substantial numbers of the root servers are owned by the US government or closely tied to it, even such an action might not suffice.

precondition to any handover of the root to ICANN.[18] The RIRs refused ICANN's draft text, however, as too one-sided in ICANN's favor and the relationship remains one in which the RIRs remain basically autonomous; while the RIRs are formally dependant on ICANN for allocations of new numbering spaces there is no realistic scenario in which ICANN could refuse reasonable requests without both causing damage to downstream parties and compromising its own legitimacy.

Despite this, however, most observers agree that currently the ultimate authority over domain names and most probably also over IP numbers belongs to the United States Government. This control owes as much to accident as it does to design. Its historic roots lie in the US government's being the paymaster for the original operators of the root, and in their subsequent desire to avoid various sorts of litigation.[19] It persists in large part because the United States retains the ultimate legal power under domestic US law to determine all changes to the root zone file, and the bodies that administer that file, and the file itself, are all located within the USA.

With narrow exceptions[20], however, the United States has delegated operational control over both internet names and numbers to ICANN, a private not-for-profit California corporation,[21] via three interlocking contracts. However, the US government also retains the effective power to terminate ICANN's influence over the Internet's infrastructure.[22]

---

[18] *See Amendment 6 to ICANN/DOC Memorandum of Understanding, at* http://www.icann.org/general/amend6-jpamou-17sep03.htm (Sept. 16, 2003) [hereinafter *Amendment 6*].

[19] *See* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17 (2000), *available at* http://www.law.miami.edu/~froomkin/articles/icann.pdf.

[20] *See* ICANN, ANNOUNCEMENT (Nov. 19, 2001)(admitting that "redelegation of .us occurred before the completion of the normal IANA requirements" -- i.e. as a result of direct action by the US government itself), *at* http://www.icann.org/anouncements/announcement-19nov01.htm.

[21]While I believe the account in the text to be both conventional and correct, it bears mentioning that it is not entirely undisputed. Certain ICANN insiders have argued that ICANN's authority is somehow not derived from the US government but rather from some free-standing consensus of the Internet community. See Joe Sims & Cynthia L. Bauerly, *A Response to Professor Froomkin: Why ICANN Does Not Violate the APA or the Constitution*, 6 J. . SMALL & EMERGING BUS. L. 65 (2002). I do not believe that the facts permit this conclusion. *See* A. Michael Froomkin, *Form and Substance in Cyberspace*, 6 J. SMALL & EMERGING BUS. L. 93 (2002), *available at* http://personal.law.miami.edu/~froomkin/articles/formandsubstance.pdf.

[22]"If DOC withdraws its recognition of ICANN or any successor entity by terminating this Agreement, ICANN agrees that it will assign to DOC any rights that ICANN has in all existing contracts with registries and registrars." ICANN, AMENDMENT 1 TO ICANN/DOC

Both the US Government's role and that of ICANN inspire controversy. As the Internet looms increasingly important in many countries' civil, artistic, and economic relations, questions increasingly arise as to the justice or legitimacy of the United States's control over the root, even if characterized as primarily a matter of stewardship akin to a government's control over a unique natural resource or cultural monument.[23] The US government has at various times pledged that when ICANN achieves certain goals the US will turn over control of the root to ICANN. Most recently, in the revised ICANN-Dept. of Commerce Memorandum of Understanding, the US stated that, "The Department reaffirms its policy goal of privatizing the technical management of the DNS in a manner that promotes stability and security, competition, coordination, and representation."[24] Some of us in the U.S., and many abroad, wonder if any Administration

---

MEMORANDUM OF UNDERSTANDING (Nov. 4, 1999) ("If DOC withdraws its recognition of ICANN or any successor entity by terminating this MOU, ICANN agrees that it will assign to DOC any rights that ICANN has in all existing contracts with registries and registrars"), *at* http://www.icann.org/nsi/amend1-jpamou-04nov99.htm. [NOTE: I am treating this document as a nonperiodic with Institutional Authors and Editors]

[23]This issue is discussed further in the WSIS section below.

[24]I*See Amendment 6, supra* note 18.

This statement must be read against a complex background. In the White Paper, DoC stated, "The U.S. Government would prefer that this transition be complete before the year 2000. To the extent that the new corporation is established and operationally stable, September 30, 2000 is intended to be, and remains, an 'outside' date." White Paper, supra note 15, at 31,744. More recently, DoC assured Congress that it intends to retain its rights over the DNS:

> The Department of Commerce has no intention of transferring control over the root system to ICANN at this time [July 8, 1999]. . . . If and when the Department of Commerce transfers operational responsibility for the authoritative root server for the root server system to ICANN, an [sic] separate contract would be required to obligate ICANN to operate the authoritative root under the direction of the United States government.

Letter from Andrew J. Pincus, DoC General Counsel, to Rep. Tom Bliley, Chairman, United States House Committee on Commerce (July 8, 1999),*available at* http://www.ntia.doc.gov/ntiahome/domainname/blileyrsp.htm

Meanwhile, or at best slightly later, DoC apparently assured the European Union that it intends to give ICANN full control over the DNS by October 2000:

> [T]he U.S. Department of Commerce has repeatedly reassured the Commission that it is still their intention to withdraw from the control of these Internet infrastructure functions and complete the transfer to ICANN by October 2000. . . . The Commission has confirmed to the US authorities that these remaining powers retained by the United States DoC regarding ICANN should be effectively divested, as foreseen in the US White Paper.

Commission of the European Communities, Communication from the Commission to the Council and the European Parliament: The Organization and Management of the Internet International and European Policy Issues 1998-2000, at 14 (Apr. 7, 2000) (emphasis added) *at*

would ever willingly surrender full control over the root, if only out of fear of being accused, however unfairly, of 'giving away the Internet.'

The US government's relationship with ICANN is also controversial domestically. Several Senators and Congressmen have raised questions about it, and there have been committee hearings on the subject. The failure to introduce legislation owes more to the absence of a convincing alternative than to any liking of the status quo. Similarly, the failure to litigate the question of the Department of Commerce's reliance on ICANN to act as its proxy regulator[25] owes more to the cost and uncertainty of litigation than any confidence that the arrangements with ICANN are strictly correct.

Even if the US were to surrender control over the root to ICANN, this might be a case of 'out of the frying pan, into the fire.' Many -- I among them -- question both ICANN's democratic legitimacy and the quality of its decisions to date.

Engineering decisions ordinarily do not require democratic legitimacy in order to command respect, but most distributional decisions do. We do not ask whether the voters have approved the tensile strength of a bridge; we ask if it is strong enough to carry the projected traffic plus a margin for safety. On the other hand, the question of where to site the bridge is both technical and political as it has distributional consequences. In democratic societies it is standard to expect that decisions with distributional consequences will be made either by elected officials or by someone ultimately responsible to an elected official. (Failure to meet this expectation is sometimes called a democratic deficit.) In addition, in democratic societies that believe themselves to be subject to the rule of law, it is standard to expect that the decisions of governing officials -- and especially bureaucrats who are not themselves elected -- will be subject to an external check such as judicial review in order to prevent arbitrary behavior and abuses of power.

ICANN originally described itself as a private body that would conduct 'technical coordination' of names and numbers. Its founders emphatically denied that ICANN was or would be a policy-maker. The nature of ICANN's activities thus determine the type of legitimacy its decisions require.[26] If its decisions are purely or even mostly technical, e.g.,

---

Recently, DoC assured the GAO that "it has no current plans to transfer policy authority for the authoritative root server to ICANN, nor has it developed a scenario or set of circumstances under which such control would be transferred." GAO Report, supra note 28, at 30. ICANN meanwhile stated on June 30, 2000, that "[s]ince it appears that all of the continuing tasks under the joint project may not be completed by the current termination date of the MOU, the MOU should be extended until all the conditions required to complete full transition to ICANN are accomplished." *Second Status Report Under ICANN/US Government Memorandum of Understanding*, § D.4, *at* http://www.icann.org/general/statusreport-30jun00.htm (June 30, 2000).

[25] *See* Froomkin, *supra* note 19.

[26] *See* Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187 (2000).

standard-setting, their legitimacy comes primarily from their correctness; the issue is largely one of quality of output and perhaps of transparency and openness. But because, as discussed below, ICANN is making frankly decisions which affect the legal relations between third parties, or which enrich or impoverish some at the expense of others, these are the sort of political choices that ordinarily call for democratic legitimation, and adherence to a more rigorous conception of due process. This agenda puts pressure on ICANN's internal structure, and especially on its accountability to the public.

The range of matters that ICANN has taken on since its creation in October 1998 (and also the potential for mission creep) can be seen by looking at its regulation of registries and registrars, the imposition (and possible amendment) of mandatory domain name dispute resolution procedures on gTLD registrants, the decision to create seven new gTLDs (and the subsequent failure to increase that number), and the ongoing debate over VeriSign's Sitefinder.

A. ICANN as Regulator

Today, there is little debate that ICANN is both a social policy-maker and regulator. The disputes, instead, concern the extent of its jurisdiction, means by which it should operate, and the degree to which ICANN should allow social policies extraneous to the technical regulation of names and numbers to determine its policies.

1. ICANN and gTLD Registries

ICANN's control over the legacy root gives it the power to control over all new registries; if they do not agree to its conditions it need not add them to the root zone file. As for the incumbent registries which pre-date ICANN, US government pressure served to force them to sign agreements giving ICANN regulatory powers over them as well. ICANN's agreements with the gTLDs impose a series of conditions on the registries, including that they agree to accept registrations only from registrars who have accepted ICANN's authority over them. Thus, ICANN's control of the root, empowers control over registries; control over registries empowers ICANN's control over registrars; and ICANN's control over registrars -- which also can be amended by ICANN -- gives it the ability to require registrars to impose contractual conditions on registrants, that is on anyone who registers a domain name in a gTLD.

In addition, ICANN retains the ability to alter its agreements with the registries. This power to amend is, however, subject to a series of procedural limits designed to ensure that ICANN's decisions regarding the registries are based on consensus. [Currently applicable policies, which were written into the original registry and registrar model contracts, were exempted from this requirement.] The procedural protections have yet to be tested, in part because ICANN has never appointed the Independent Review Panel whose existence is a precondition to ICANN's invoking its power to compel a registry to adhere to a "consensus policy" adopted by the Board.

ICANN's power over registries and registrars in the gTLD market means that like it or not, a side effect of any rule ICANN makes has an impact on the structure of the market for domain names. ICANN has so far resisted focusing on the economic consequences of its decisions, other than to site the need for 'stability' as one reason to keep down the level of competition between gTLDs. ICANN seems to believe that one of its duties is to prevent any

gTLD from failing, a view that has obvious implications for its willingness to increase competition among gTLDs. (In contrast, ICANN has been willing to permit nearly unlimited competition among registrars since when one fails the data needed to resolve domains to IP numbers and to establish the party responsible for the domain remains with the registry.[27])

Thus, although the full extent of its power to alter the contracts remains to be tested, ICANN is the de facto regulator of the terms of service for gTLD registries. (This authority is of course exercised coterminously with the local law of the place where the registry is located.) Currently ICANN uses this power to regulate prices, services, and terms of services for gTLD registries and (for all but the price of registration services) registrars. ICANN does so in a legal environment that characterizes what is in effect regulation as contract. This characterization makes judicial review of ICANN's regulatory choices all but impossible.

2. ICANN and ccTLDs

ICANN's power over ccTLDs is in principle far more constrained than its power over gTLDs. The ccTLDs pre-date ICANN. The US government may have pushed NSI/VeriSign to sign agreements with ICANN, but its attitude towards the ccTLDs has been far more deferential. Since its inception, ICANN has sought to encourage, even coerce, ccTLDs to sign contracts[28] promising to pay fees to ICANN and to accept its regulatory authority. Most have refused. According to ICANN's ccTLD page, http://www.icann.org/cctlds/agreements.html, only ten have signed agreements with ICANN to date, several after ICANN -- with the consent or encouragement of the local government -- replaced the previous ccTLD administrator.[29] ICANN has not asserted a power to regulate the ccTLD's operations equivalent to the power it exercises over gTLD registries.

Nevertheless, ICANN's relationship with ccTLDs exhibits three potentially worrying aspects. First, ICANN has not been shy about using its "IANA" power to re-assign ("re-delegate") ccTLDs. All of these re-delegations are conducted in secret. Although many of these decisions have not been controversial, some have been, notably the decision to re-delegate .au from an Internet pioneer to an ICANN-like entity created by the Australian government. The Australian incident was particularly suspicious: acting under pressure for the Australian government, a major source of moral and financial support for ICANN's GAC activities, ICANN re-delegated .au in violation of its own, somewhat skimpy, rules.[30]

---

[27]One exception to this rule is if the registrar and registry are the same body.

[28]*See* http://www.icann.org/cctlds/model-mou.html.

[29]For a list of redelegations see IANA, *INIA Reports About ccTLDs, at* http://www.iana.org/cctld/cctld.htm#IANAReports.

[30]*See* A. Michael Froomkin, *How ICANN Policy Is Made (II, at* http://www.icannwatch.org/essays/dotau.htm (Sept. 5, 2001).

Second, ICANN's re-delegations seem to be connected to the willingness of the new recipient of a ccTLD to sign ICANN's model ccTLD contract,[31] an agreement that obligates the ccTLD to pay what are in effect taxes to ICANN, and allows ICANN to raise these by as much as 15% per year. Indeed, the .au re-delegation was immediately followed by the new Australian ccTLD operator becoming the first to conclude an agreement with ICANN on ICANN's terms.

Last, and perhaps most worrying, ICANN's recent behavior towards truculent ccTLDs demonstrates that ICANN remains willing to use its muscle to expand its power. ccTLD administrators mistrustful of ICANN are unwilling to allow it to copy their data. If ICANN were in possession of their data, it could replace them and turn the data over to the ICANN-selected successor. Without its predecessor's data, the successor would be unable to run the registry since it would not know which names were registered, and by whom. Last year it emerged that ICANN was in effect blackmailing ccTLD administrators who refused to sign agreements with it, or to allow ICANN to copy their critical data, by neglecting to process their requests for routine changes to their name server records in the root zone files.[32] In this case, the US government came to the rescue by making the prompt servicing of these routine requests a condition of its renewal of ICANN's authority to conduct the IANA function.[33]

In forcing ICANN to provide better service to ccTLDs, the US government was likely responding to pressure from other governments. Indeed, governments appear to be taking an increasing interest in the functioning of their domestic ccTLD. The recent ITU-sponsored ccTLD study by Prof. Michael Geist study found that,

> • Governments are deeply involved in domain name administration at the national level. Contrary to most expectations, virtually every government that responded either manages, retains direct control, or is contemplating a formalized relationship with their national ccTLD.
> • 47 percent of responding governments retain ultimate control over their national ccTLD. A further 25 percent have taken specific steps toward asserting ultimate authority over their national ccTLD. Twenty percent of respondents indicated that they were considering formalizing their relationship with their ccTLD and expected that relationship to change in the future. Only seven percent of

---

[31] *See* David Post, *The Other Shoe Drops, II (or III,…), at* http://www.icannwatch.org/article.pl?sid=01/10/26/094629 (Oct. 26, 2001).

[32] Nominet's (the UK ccTLD adminstrator) angry reaction, http://www.icannwatch.org/article.pl?sid=02/11/19/120332, is perhaps typical

[33] *Contract Between ICANN and the United States Government for Performance of the IANA Function,* § C.2.1.1.2, *at* http://www.icann.org/general/iana-contract-17mar03.htm (Mar. 17, 2003). The IANA contract is more than usually opaque as it is formally a purchase order by the US government of IANA services from ICANN -- for $0. In fact, this "purchase" is the lynchpin of ICANN's authority.

respondents indicated no formal governmental role in their ccTLD with no plans to alter the present situation.[34]

Thus, with the exception of the small number of ccTLDs that have concluded agreements with ICANN and thus granted it a measure of control on par with that exercised over gTLDs, ccTLD regulation remains almost entirely a matter for the domestic authorities in the state where the ccTLD is located.[35]

3. ICANN and new TLDs

Nowhere is ICANN's regulatory power more obvious than its gatekeeper role regarding the creation of new TLDs. ICANN was supposed to set up a process by which new TLDs might be created. The creation of new TLDs has a technical component, but also has large distributional consequences.

The technical aspects of the new TLD issue include defining what is required to operate a registry (e.g. access to what sort of hardware, software, resources), which existing Internet standards must be adhered to (primarily IETF RFC's relating to the DNS), and perhaps requiring clear rules for the delegation of domain names within the TLD. In particular, there is a technical aspect to the initial "landrush" period when a TLD opens; for a popular TLD there may be many applicants seeking a particular name, and the new registry needs to be prepared to allocate them quickly and, ideally, fairly.

The new TLD issue also has more visibly political aspects. First, while it may be possible to create an unlimited number of new TLDs, this is not certain. The question of how many to create and when is thus both technical and political. If the potential number were very small, it would be irresponsible to use up all of the depletable resource at once; on the other hand, the failure to create new and attractive TLDs allows first-movers to entrench themselves into the marketplace. Indeed, incumbent TLD registries have sought to minimize the entry of potential competitors, and to ensure that any new entrants are structured in a way that limits their market appeal (for example, a "sponsored" TLD such as .aero will likely pose much less of a competitive threat to .com than would, say, .web).

As noted above, opinions differ on the maximum number of new TLDs that would be safe, but there is a near-universal consensus that hundreds more would pose no danger so long as they were introduced incrementally. In its approximately five years of life, however, ICANN has authorized only seven new TLDs, many of them of quite limited appeal. It has run only one iteration of the application process, culminating in November 2000. The selection process was justly criticized for being needlessly expensive, cumbersome, intrusive on the commercial and social choices of the applicants, and highly arbitrary. Strikingly, ICANN abandoned all pretense

[34]Michel Geist,*Governments and Country Code Top Level Domains: A Global Survey*, *at* http://www.michaelgeist.ca/geistgovernmentcctlds.pdf (2003).

[35]By longstanding rule predating ICANN, the administrator of a ccTLD is required to be resident in the state to which that country code refers.

of making technical judgments and instead held what amounted to a comparative hearing in which it focused less on the technical capacity of applicants, and more on the names they proposed to use, their business plans, and the perceived social utility of the proposals. The defining moment of the hearings may have been when the Board voted to reject an applicant at the eleventh hour because its proposed TLD, ".iii" was "too hard to pronounce"--a criterion never before mentioned at any stage in the process. ICANN also rejected ".union" -- proposed by an international consortium of well-established labor organizations -- on the grounds that it was unable to determine if this group was sufficiently representative of the workers of the world.

The disappointed applicants from that first process, each of whom paid a US$50,000 application fee more than three years ago, remain officially on hold to this day. ICANN has at various times suggested it plans a moratorium on all TLDs, or all but limited-appeal "sponsored" TLDs, or would open up applications to newcomers, or would put the entire process on hold until it could draft new rules for its selection decisions. Academic experts have proposed such plans,[36] but ICANN has to date shown little enthusiasm other than occasional lip service, for any plan that would produce rapid and predictable decisions at the expense of its current standardless discretion (or stasis).

4. ICANN's UDRP

Using its power to impose terms on registrars, ICANN requires all registrars in the legacy root to in turn impose a mandatory arbitration clause on all registrants to .com and other "global" TLDs (gTLDs) that are not linked to any particular country. The clause can be invoked by anyone, anywhere, who thinks that his trade or service mark is infringed by a second-level domain name registered in a gTLD. The UDRP is popular with mark holders, who find it quick and relatively cheap. The UDRP's goals were to provide a rapid and inexpensive means of vindicating rights that were clear under the relevant national law.

The substance of the UDRP has been somewhat erratically applied by the small group of arbitration service providers, but overall there has been general acceptance of the substantive aspects of the UDRP except as applied to marks that allegedly have protected expressive aspects, where some, but not all, commentators say that the UDRP (or the arbitrators applying it) fails to give due consideration to the expressive rights of non-commercial users seeking to criticize corporations by hosting web sites with derogatory domain names (e.g. "companysucks.com").

The procedural aspects of the UDRP, however, have been criticized by the majority of academics who have studied them for lacking procedural due process and for exhibiting basic structural biases. As it stands, the UDRP has a large number of obscure but significant procedural defects. Because of these, the system fails to guarantee basic due process to consumers who register domain names. In addition, serious questions have been raised about the even-handedness of some of the arbitration service providers who supply the arbitrators for the UDRP; as currently written, the UDRP creates economic incentives for arbitration providers to

[36] *See, e.g.,* Karl Manheim & Lawrence Solum, An *Economic Analysis of Domain Name Policy*, 25 HASTINGS COMM. & ENT. L.J. 359 (2003), *available* at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=410640.

be "plaintiff-friendly," and to discriminate subtly against consumers. Service providers' are not required to disclose their methods of recruiting and assigning arbitrators, and the system permits provider manipulation of panelist selection to achieve a desired result in a given type of case.[37]

[37]Here is my personal list of criticisms, adapted from A. Michael Froomkin, *ICANN's "Uniform Dispute Resolution Policy" -- Causes and (Partial) Cures*, 67 BROOK. L. REV. 605 (2002), *available at* http://personal.law.miami.edu/~froomkin/articles/udrp.pdf. :

Basic Fairness Issues

- The UDRP contains incentives for arbitration providers to be 'plaintiff-friendly';
- There is no forum in which plausible claims of arbitration-provider bias can be heard;
- Parties need an enhanced means to get information about arbitrators' possible conflicts of interest and to act on that information;
- In order to discourage frivolous complainants, complainants should be required to post a small bond that would be forfeited in the event of a finding that the complaint was brought in bad faith and constitutes an abuse of the administrative proceedings;
- Consumers do not always have access to an authoritative copy of the UDRP in their national language;
- Providers' methods of recruiting and assigning arbitrators should be open and auditable to avoid tempting providers to manipulate panelist selection;
- Complaints and replies should be published online along with decisions in order to increase confidence in the justice of outcomes, subject to redaction of confidential business information which should be segregated in limited exhibits. Providers should be required to archive all briefs and exhibits for several years, and to make them available after a reasonable time to researchers and others who want to study them, with some provision for redaction of the most sensitive personal and financial data.

Practice and Procedure Under the UDRP

- There is uncertainty about what suffices to meet the complainant's burden of proof;
- The UDRP should specify that neither settlement negotiations nor solicited offers of sale constitute evidence of registrant bad faith;
- Either the UDRP should spell out in some detail what sort of evidence will be considered proof of the existence of a common law mark, or the UDRP should be limited to registered marks;
- UDRP decisions should be final within the system -- any complaint that elicits a reply should not be subject to a "dismissal without prejudice" that invites complainants to try and try again;
- The UDRP should not allow parties even to attempt to undermine a final decision on the merits by a court of competent jurisdiction;
- The rules should require actual notice or greater efforts reasonably calculated to achieve actual notice, especially in countries with inferior postal systems;
- Complainants should be penalized for filing lengthy attachments and exhibits in an attempt to evade word limits, and for submitting most non-digitized material.
- More investigation is needed into the causes of the high rate of default judgments and the extent to which these cases are being decided fairly.

a. WIPO2

ICANN is currently considering a request from the World Intellectual Property Organization (WIPO) that it extend the reach of the UDRP to protect country names and the names of international organizations, neither of which is protected under trademark law, at least in the United States.[38]

At present the UDRP protects only trade and service marks, so the extension to para-trademark rights would be a precedent of some significance. The so-called WIPO2 proposal also asks that the UDRP be amended to excuse both nations and international organizations from having to consent to suit in a national court (which requires that they waive their sovereign immunity) if they win the UDRP proceeding. Instead it proposes that they agree to be subject to a traditional international arbitration -- a very mixed blessing for individual litigants, who will have to pay the tribunal as well as their lawyers, and may not get a judge as familiar with their traditions as they would if the case were tried in their home court.[39]

ICANN has set up a committee to advise the Board on these questions.[40] The committee is due to submit a report early next year, one which the Board is free to accept or ignore.

b. Reform of the UDRP? Or Ossification?

Long before the WIPO2 proposal arrived, ICANN had promised to review the functioning of the UDRP. The promised review was late in coming, but eventually a committee was appointed. It then collapsed without issuing a report. After this debacle, this past August the ICANN Staff Manager posted an Issues Report on UDRP Review.[41] The Report is most notable for its vision of the procedural environment constraining any attempt to amend the UDRP. It suggests that where national laws vary, and harmonization is not feasible, ICANN should consider the substantive question as beyond ICANN's scope because it may not be possible to make a consensus policy. The report describes the UDRP as a consensus policy (it is defined as such in the registry contracts although not developed as one) that may only be changed by consensus.

Johnson and Crawford, often sympathetic observers of ICANN, criticized this stance as leading to paralysis:

---

[38]International organizations that do business under their name are protected. Flags and insignia of countries also have protection.

[39]Venue in the post-UDRP case is either the home of the registrant or the registrar, and the complaining party can choose between these if they are different.

[40]I represent the non-commercial constituency on this committee.

[41]*Staff Manager Issues Report on UDRP Review, at* http://www.icann.org/gnso/issue-reports/udrp-review-report-01aug03.htm (Aug. 1, 2003).

> If taken seriously, this analysis would launch ICANN towards a future in which (1) it cannot create new substantive policies and (2) it cannot abandon the policies that exist now only because the DOC (or ICANN staff) insisted on them when initial (non-negotiable) contracts were drafted. This is an unstable and ultimately destructive direction for ICANN to take.[42]

Whether the Staff Manger paper is the sign of a new, far more modest, regulatory strategy or an aberration remains to be seen. On the one hand, an ICANN that for the first time took the consensus requirement seriously would thereby defang almost all the legitimacy questions that have dogged it since its inception. On the other hand, the result would be to freeze in place existing policies such as the UDRP that have some substantial flaws.

5. Site Finder: Core Mission or Mission Creep?

The presence of (near) consensus can be almost as dangerous as its absence. On Sept. 15, 2003, VeriSign -- the registry for .com and .net -- unveiled its new "Site Finder" service. Henceforth, all attempts to reach a domain lacking a listing in the registry would no longer receive a "not found" error but instead a page of 'helpful' suggested sites, including links marketed by VeriSign.[43]

The technical community's response, and indeed that of much of the Internet community, was vitriolic. VeriSign's surprise change broke assumptions on which many esoteric, and a few less esoteric, Internet applications were based. It violated the spirit if perhaps not the letter of the governing Internet Standards issued by the IETF. The authors of BIND, the most commonly used DNS software quickly issued a patch which disabled Site Finder, but at least the first version of the patch created a few problems of its own, and as Jonathan Weinberg documents,[44] the patch did not meet with mass acceptance immediately.

Whether a technical solution would have worked in the longer term is unclear, as VeriSign turned off Site Finder three weeks after turning it on, upon receipt of a "formal demand" from ICANN that it do so. In the demand, ICANN threatened to find VeriSign in breach of its registry contracts unless VeriSign capitulated, vowing to revive Site Finder once it had worked out more of the bugs.

While ICANN's action was wildly popular in the Internet community, its legal position was formally dubious. As Jonathan Weinberg argues, VeriSign in fact had no obligation to comply with ICANN's new policy banning wildcards because ICANN failed to create the

---

[42] David R. Johnson & Susan P. Crawford, *ICANN's Newest Catch 22*, *at* http://www.icannwatch.org/article.pl?sid=03/08/04/0121221 (Aug.3, 2003).

[43]The best account of this affair to date is Jonathan Weinberg, *Site Finder and Internet Governance*, *at* http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID475281_code70168.pdf?abstractid=475281 (20030).

[44]*See id.*.

Independent Review Panel whose existence is a condition precedent to its enforcement of controversial policies.[45] Nor, he shows, is it at all clear that on these facts ICANN had the contractual ability to find VeriSign in breach, although the issue is not completely clear-cut. Lacking breach, ICANN would have no way to credibly threaten to refuse to renew VeriSign's registry contracts when they expired.[46]

One could conclude from this that if ICANN lacks the tools to respond even to a self-interested, possibly destructive, fundamental change in basic Internet architecture, then ICANN is too weak. Prof. Weinberg himself flirts with this conclusion. But he also notes powerful counter-arguments, among them that overall ICANN already intrudes too much into the business methods and services of registrars and registries to the detriment of competition. Coupled with ICANN's democratic deficit and the ironic fact that the main reason a change to .com is so devastating to the Internet generally is that ICANN's own policies have stifled the growth of plausible alternative domains. In the end, the most he is willing to say is that,

> there needs to be an effective institutional mechanism for protecting the domain name space infrastructure from unilateral, profit-driven change that bypasses the protections and consensus mechanisms of the traditional Internet standards process. Notwithstanding ICANN's flaws, it may be better suited than any other existing institution to protect against that threat. Yet ICANN regulation is itself highly problematic, and so any plan to expand its authority must be approached with care.[47]

B. Internal Governance

Despite a rhetoric of 'bottom up' organization and empowerment, the reality is that the majority of the ICANN Board has always had the power to do more or less what it wants. At times it has delegated this power to its staff, at times the staff and the Board majority have tried to freeze out a dissident director,[48] but none of this changes the basic fact that the ultimate determinant of ICANN policy is votes on the Board.

1. Board Composition

---

[45] *Id.* at 18-19.

[46] *Id.*. at 19-20.

[47] *Id.* at 1

[48] See Auerbach v. ICANN, No. BS074771 (L.A. Super. Ct. Cent. Civ. Div. July 29, 2002) (holding that ICANN must give dissident director access to its files), *at* http://www.icannwatch.org/essays/auerbach-tentative-ruling.pdf.

The latest iteration of the ICANN Bylaws,[49] a product of a protracted 'reform' process, works substantial changes over their more than a dozen (in less than five years!) predecessor versions. The three most important changes are: (1) The "new bylaws that allow the Board to adopt domain name policies by a vote of the Board, irrespective of the presence or absence of consensus among any of the various stakeholders. These new bylaws represent an intentional departure from the consensus decision-making model, and a move towards centralized, top-down policy-making."[50] (2) The Board gains increased power to perpetuate itself, and removes all traces of end-user control over the selection of Board members--including the somewhat maligned ICANN electronic voting procedure that formerly chose about a third of the Board. (3) The influence of government representatives via ICANN's shadowy "Government Advisory Committee" substantially increases.

The clear losers from the reform are end-users of domain names, especially individual registrants. The original ICANN bylaws reserved nine of nineteen director positions for at-large members who were supposed to represent the public. ICANN's initial incorporators named all nine, five of whom where then replaced by elected directors, with 160,000 individual Internet users registered as ICANN members eligible to cast votes. Later, a committee chaired by former Swedish Prime Minister Carl Bildt proposed to reduce the number of at-large directors to six and to allow only domain name holders to participate in elections. The current 'reform' however provides for no direct Internet user representation on the Board. Their representatives are consigned to an advisory committee (the ALAC[51]), but even there they are indirectly elected. Instead, the Board perpetuates itself by selecting a "nomcom" which in turn selects the majority of ICANN's Board members.[52]

---

[49]ICANN, BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (2002), *available at* http:// www.icann.org/general/bylaws.htm [hereinafter *Bylaws*].

[50]David R. Johnson et al.,, *A Commentary On The ICANN "Blueprint" For Evolution And Reform*, 36 LOY. L.A. L. REV. 1127 (2003).

[51]ALAC will have a non-voting liaison to the ICANN Board and will name five members to the Nominating Committee. The ALAC can also offer advice to the Board; however, unlike advice from the GAC, the Board is not obliged to take ALAC's advice into consideration or to publicly explain why it has ignored ALAC's advice. *Bylaws, supra* note 49, at art. XI § 2.4.e.

[52]See http://www.icann.org/committees/nom-comm/. Government representatives influence the selection of Board members via their participation in the NomCom. *See Bylaws, supra* note 49, art. XI, § 2.1.j. Initially five of the eighteen voting members of the NomCom will be picked by the ALAC, which is the group that represents the public. Of the remaining thirteen seats on the NomCom, six represent various business groups, three represent technical groups, and one seat represents each of consumer, governments, ccTLDs, and academic and noncommercial interests. *See id.* art. VII, § 2; *see also* ICANN, FINAL IMPLEMENTATION REPORT AND RECOMMENDATIONS OF THE COMMITTEE ON ICANN EVOLUTION AND REFORM §§2.B, 3.E (Oct. 2, 2002) (giving reasons for the proposed structure of the Board and NomCom), *at* http://www.icann.org/committees/evol-reform/final- implementation-report-02oct02.htm.

2. New role of GAC in ICANN

Direct representation of end-users vanished, but direct representation of governments appeared. Where formerly ICANN was explained as "privatized" Internet governance, now its description of itself states among its "core values," is "remaining rooted in the private sector, recognizing that governments and public authorities are responsible for public policy and duly taking into account governments' or public authorities' recommendations."[53] ICANN had originally hoped to seat a minority of government delegates on its Board in exchange for direct financial subsidies, but the governments were unwilling to agree to this. As it worked out, they may have gotten more control, for a much lower cost.

Governments now directly influence ICANN via the Government Advisory Committee, a body made up of representatives of all interested governments -- approximately 75 have participated at one time or another -- plus a small number of delegates from international bodies (WIPO, ITU). Formerly a truly advisory body (on paper at least), GAC now has direct powers to influence ICANN's decisions. To begin with, the GAC sends a non-voting liaison to the Board.[54] The GAC liaison attends all Board meetings, including the ones closed to the public -- but no one outside the GAC itself attends the GAC's meetings. The ICANN Board can remove non- voting liaisons from other advisory committees, but not the GAC liaison.[55] (The GAC also has the right to send non-voting liaisons to all other ICANN advisory committees and supporting organizations, allowing it to become involved in all phases of the policy development process.)

GAC makes recommendations that cannot easily be ignored. The Board must take GAC recommendations "duly . . . into account, both in the formulation and adoption of policies."[56] Should the Board reject a GAC recommendation, it must not only "inform the [GAC] and state the reasons why it decided not to follow that advice"[57] but also enter into further negotiations with the GAC "to find a mutually acceptable solution.."[58] If at the end of the day "no such solution can be found, the ICANN Board will state in its final decision the reasons why" it did not do what GAC instructed.[59]

---

[53] *Bylaws, supra* note 49, art. I, § 2.11.

[54] *Id.* art. I, § 2.11.

[55] *Id.* art. VI, § 11.2. If the Board wishes to remove the GAC liaison, three-fourths of the directors must vote to request that the GAC consider appointing a different liaison.

[56] *Id.* art. XI, § 2.1.j.

[57] *Id.*

[58] *Id.*

[59] *Id.* art XI, § 2.1.k.

ICANN's Board must "notify the Chair of the Governmental Advisory Committee . . . of any proposal raising public policy issues on which it or any of ICANN's supporting organizations or advisory committees seeks public comment, and shall take duly into account any timely response to that notification prior to taking action."[60]

The GAC can also raise issues on its own: it "may put issues to the Board directly, either by way of comment or prior advice, or by way of specifically recommending action or new policy development or revision to existing policies."[61]

As Wolfgang Kleinwoechter states, "An unusual relationship now exists between ICANN, the private corporation with the responsibility of managing a core resource of the global Internet, and the governments of the United Nations. This relationship resulted from political and diplomatic battles between private Internet stakeholders and the U.S. government, and between the U.S. government and other governments, in particular the European Commission and the ITU."[62]

IV. Trade Treaties and ICANN

Spurred by its commitment to the protection of intellectual property, the United States has been encouraging other nations to enter into treaty commitments that would bind them to implement whatever rules ICANN adopted in its UDRP. Thus, for the Free Trade Area of the Americas, the United States proposed that the Intellectual Property chapter include,

> [13.1. Each Party shall participate in the Government Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) to promote appropriate country code Top Level Domain (ccTLD) administration and delegation practices and appropriate contractual relationships for the administration of the ccTLDs in the Hemisphere. Each Party shall have its domestic Network Information Centers (NICs) participate in the ICANN Uniform Dispute Resolution Procedure (UDRP) to address the problem of cyber-piracy of trademarks.]

Similar language already appears in bilateral trade agreements the US has concluded with Chile and Singapore, and the US Dept. of Commerce has pledged to seek to include it in future bilaterals.[63]

---

[60] *Id.* art. XI, § 2.1.h.

[61] *Id.* art. XI, § 2.1.i.

[62] Wolfgang Kleinwoechter, *From Self-Governance To Public-Private Partnership: The Changing Role Of Governments In The Management Of The Internet's Core Resources*, 36 LOY. L.A. L. REV. 1103 (2003).

[63] See *Internet Domain Name Fraud—The U.S. Government's Role In Ensuring Public Access To Accurate Whois Data, Hearing Before The House of Representatives Subcommittee On Courts, The Internet, And Intellectual Property Of The Committee On The Judiciary*, 108th

As a matter of international law, these are peculiar clauses to put into any treaty. They commit the signatories to impose ICANN's UDRP on the users of their ccTLDs, who will primarily be their own citizens. As ICANN already imposes the UDRP on all registrants in gTLDs such as .com, and no action is required to maintain the status quo in this regard. Thus, the citizens' legal rights are made subordinate to a private corporation. (And, if the national ccTLD registry is private, a domestic corporation is subjected to regulation by a foreign one.) ICANN can change the UDRP at any time. Indeed, as noted above discussions are currently under way to expand the reach of the UDRP. Even nations satisfied with the UDRP as it stands at present, may find themselves locked into a system that might change in ways they find objectionable.

V. World Summit on the Information Society (WSIS)

As noted at the outset of this paper, there is a potential mis-match between governments' ambitions to regulate internet-mediated conduct (and even expression) and the ability of those governments to achieve their aims by purely national regulation. That the Internet enables regulatory arbitrage, and that national rules thus have greater spillover effects than previously are now familiar phenomena.

Some may be tempted to turn to ICANN to help regulate cross-board internet activities. But as demonstrated by ICANN's difficulty in articulating a justification for regulating even core architectural issues such as Site Finder, and as further confirmed by its legitimacy problems, ICANN is a poor tool for resolving jurisdictional and regulatory problems, especially when the problems are designed to achieve ends outside the sphere of direct regulation of internet infrastructure.

Frustrated by their inability to regulate activities with consequences within their borders, or frustrated because they have not been regular participants in GAC and are not among the ICANN 'insiders' -- reputed to be the US, the EU, and Japan -- many nations have sought alternate strategies for finding leverage over Internet activities. The ICANN lesson that much in other spheres can be leveraged from control of the infrastructure has not been lost on these nations, and they have therefore started exploring which parts of the ICANN functions might be transferred to the UN, the WTO, or perhaps to some new multilateral treaty body. These initiatives, however, are likely to meet resistance from those nations -- perhaps mindful of the unlamented attempt in UNESCO in the early 1980s to create a New World Information Order

---

Cong. (Sept. 4, 2003) ("The Department is also addressing these issues in bilateral free trade agreements by advocating that these agreements include commitments by governments that their country code top level domain operators will provide WHOIS-type registrant information and a cybersquatting dispute resolution procedure. As a result of this advocacy, such provisions were included in the free trade agreements between the United States and Singapore and the United States and Chile."), *at* http://commdocs.house.gov/committees/judiciary/hju89199.000/hju89199_0.htm.

regulating news organizations -- that are unwilling to entrust any control over their domestic communications to an international body.

These conflicting views came to a head in the negotiations prior to the World Summit on the Information Society (WSIS). As the BBC reported,

> Developing nations had been pushing for the UN to have a far greater role in the regulation of the net, while western countries opposed handing over control to an international agency.
>
> Negotiators side-stepped their differences by putting the issue on the back-burner.[64]

Indeed, the draft (v.3, Dec. 9, 2003) Declaration of Principles, appears to put off the most contentious questions until the Tunis meeting in 2005:

> 48. The Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.
>
> 49. The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:
> a) policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;
> b) the private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;
> c) civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role;
> d) intergovernmental organizations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues;
> e) international organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.
>
> 50. International Internet governance issues should be addressed in a coordinated manner. We ask the Secretary-General of the United Nations to set up

[64] BBC, GO AHEAD FOR UN INTERNET SUMMIT (Dec. 8, 2003), *at* http://news.bbc.co.uk/2/hi/technology/3300071.stm.

> 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.[65]

As for the accompanying Draft Plan of Action, it asserts the leading role of governments in the formation of Internet policy...

> Governments have a leading role in developing and implementing comprehensive, forward looking and sustainable national e-strategies. The private sector and civil society, in dialogue with governments, have an important consultative role to play in devising national e-strategies.[66]

...but commits them only to a set of fairly vague activities...

> a) Governments should foster a supportive, transparent, pro-competitive and predictable policy, legal and regulatory framework, which provides the appropriate incentives to investment and community development in the Information Society.
>
> ...
>
> c) Governments are invited to:
> i) facilitate the establishment of national and regional Internet Exchange Centres;
> ii) manage or supervise, as appropriate, their respective country code top-level domain name (ccTLD);
> iii) promote awareness of the Internet.
>
> d) In cooperation with the relevant stakeholders, promote regional root servers and the use of internationalised domain names in order to overcome barriers to access.[67]

---

[65]ITU, DRAFT DECLARATION OF PRINCIPLES (Dec. 9, 2003), *at* http://www.itu.int/dms_pub/itu-s/md/03/wsispc3/td/030915/S03-WSISPC3-030915-TD-GEN-0006!R3!MSW-E.doc.

[66]ITU, DRAFT PLAN OF ACTION § A. 3(Dec. 9, 2003), *at* http://www.itu.int/dms_pub/itu-s/md/03/wsispc3/td/030915/S03-WSISPC3-030915-TD-GEN-0005!R3!MSW-E.doc.

[67]*Id.* § C6.13.

Exactly what this will mean in practice is hard to say. Much of it is vague, although the definition of the Internet as a "global facility" is code for making it a matter of public regulation rather than private management,[68] *"Shaping Information Societies for Human Needs"*, § 2.4.7, Civil Society Declaration to the World Summit on the Information Society, Unanimously Adopted by the WSIS Civil Society Plenary on 8 December 2003, available online at http://mboom.draper.albany.edu/%7Emciver/WSIS/CSDeclaration/Summit/Final/WSIS-CS-Decl-08Dec2003-eng.txt and tends to be used to invoke regulation by something akin to the ITU.

In contrast, the Draft Plan of Action gives the UN Secretary General a relatively direct instruction to prepare a study and promote clarity:

> b) 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. The 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.[69]

---

[68] An alternate vision was provided by the civil society representatives:

> In light of the relevant controversies in the WSIS process, special attention must be given to improving the global coordination of the Internet's underlying resources. It must be remembered that the Internet is not a singular communications "platform" akin to a public telephone network; it is instead a highly distributed set of protocols, processes, and voluntarily self-associating networks. Accordingly, the Internet cannot be governed effectively by any one organisation or set of interests. An exclusionary intergovernmental model would be especially ill suited to its unique characteristics; only a truly open, multistakeholder, and flexible approach can ensure the Internet's continued growth and transition into a multilingual medium. In parallel, when the conditions for system stability and sound management can be guaranteed, authority over inherently global resources like the root servers should be transferred to a global, multistakeholder entity.

[69] ITU, *supra* note 66, § C6.13.

This falls far short, however, of justifying the claim that the "UN has been given until 2005 to take control of the digital highway."[70]

VI. Other Regulatory Methods Available to National Governments

Were a multilateral treaty solution to materialize, or one grounded in an existing international organization, it would offer the promise of a truly global solution to problems of domestic and transnational regulation of internet issues as the transnational control of internet infrastructure could be used to empower domestic regulators. In the short term at least, no such solution seems likely.

Governments are far from powerless however. They have a large number of traditional regulatory tools at their disposal. With the exception of a very few notorious cases such as in South Africa,[71] governments have had little difficulty regulating their national registries, and even in the more recalcitrant cases the local administrator has had to give in in the end. Many of the traditional regulatory tools can be focused on end-users, or on intermediaries such as ISPs. When they cannot, governments have demonstrated that they can negotiate and even conclude more specific multilateral agreements that deal with individual aspects of Internet regulation, e.g. cybercrime, cross-border sales, or money laundering.

Governments have also only begun to exploit their ability to require that devices sold within their jurisdiction be designed to facilitate regulation. The 'trusted computing' initiative[72] and the 'broadcast flag'[73] are only the first signs of hardware-based trends that could, if they continue, make ICANN's contract-based regime of Internet regulation, and even the hypothetical treaty or UN-based regulatory systems, seem quite tame.[74]

---

[70]The claim appears in an African news story at the ordinarily reliable allafrica.com. The full quote is:

> The transference of Internet governance from US corporation ICANN (Internet Corporation for Assigned Names and Numbers) to the United Nations has been viewed as one of the biggest victories for the developing world. The UN has been given until 2005 to take control of the digital highway.

WSIS Declaration Nearly Complete, http://allafrica.com/stories/200312090813.html.

[71]*See, e.g.*, ICANNWatch, *.za Zone File Expatriated, at* http://www.icannwatch.org/article.pl?sid=02/06/13/200805 (June 13, 2002).

[72]See Ross Anderson, *`Trusted Computing' Frequently Asked Questions, at* http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (Aug. 2003).

[73]The Broadcast Flag is an FCC-mandated program that requires consumer devices capable of receiving broadcast digital television (DTV) signals to implement content control technologies demanded by the entertainment industry by July 1, 2005.

[74]See A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000), *available at* http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

Conclusion

ICANN's recent reforms cemented its internal position. There is no longer a meaningful internal opposition to the ICANN Board majority, or to the staff. There are no more dissident directors such as Karl Auerbach. There are no elections for public directors. To date this has not resulted in any great change in the snail's pace with which ICANN moves on issues such as new gTLDs, and indeed there are some indications, such as the Staff Manager's Report on the UDRP, that ICANN is reconsidering its ability to act at all in the absence of (very rare) consensus. If ICANN waits for consensus, it may be paralyzed. If it does not, the self-selected nature of the ICANN Board and the absence of meaningful external checks on its actions (other than the unwillingness of the RIRs and the ccTLDs to acknowledge ICANN's authority) will continue to cast a long shadow over ICANN's legitimacy. In the end, an activist ICANN that attempted to regulate beyond a narrow range of infrastructural issues would be even more certainly doomed than a passive ICANN, but fate can take a long time to work itself out. There may be a middle ground between those alternatives, but it is a narrow ground indeed.

As a result of ICANN's reforms, governments now have more power than ever before over ICANN's affairs. Governments exercise this power by acting through the GAC -- a body whose status as an international governmental advisor to a private US corporation may be unprecedented. Equally unprecedented is the elevation of the rules produced by a private corporation to something that nations are obligated by treaty to enforce on their citizens. Yet, even while they influence ICANN and subject themselves to it, governments, paradoxically, are also the greatest threat to ICANN. The threat manifests itself in two contradictory ways. The internal threat is that governments will abuse the ICANN process in order to secure advantages outside the sphere of infrastructure regulation. The WIPO 2 process -- in which governments seek new para-trademark protection for their names and for the names of the multinational bodies they set up -- can be seen as the first, relatively mild, example of this. The external threat is that governments will become impatient and try to replace ICANN with any of a panoply of alternatives that are difficult to implement but would be even harder to dislodge. ICANN has been very far from an ideal regulator of the portions of the internet infrastructure under its purview, but there is little reason to believe as yet that any of the most likely alternatives are preferable.