Political Oversight of ICANN: A Briefing for the WSIS Summit

Concept Paper by the
Internet Governance Project
www.internetgovernance.org

1 November, 2005

"Political Oversight" of ICANN:

A Briefing for the WSIS Summit[1]

As the UN World Summit on the Information Society (WSIS) approaches its final meeting, political oversight of Internet governance has become the paramount issue. It has also proven to be a politically charged and divisive issue, making it impossible for the 3rd Prepcom to reach an agreement.

In this document we attempt to provide conceptual clarity on issues relating to political oversight. We first define political oversight and briefly assess why it might or might not be needed for international Internet governance. Next, we make an important distinction between *narrow oversight* (of ICANN) and *broad oversight* (of all Internet public policy issues), and explain why WSIS must separate discussion of these two types of oversight.

We then examine in detail the existing mechanisms of political oversight over ICANN. We note that unilateral U.S. oversight is troublesome and needs to be changed. But there are two very different ways to do this. One way is to bring more governments into the supervisory process. Another way is to remove the U.S. government from the picture. In other words, one can *de-nationalize* ICANN and find ways of making it accountable that do not require traditional inter-governmental supervision.

The paper concludes that de-nationalization is probably a better option than internationalization. Moreover, the existing mechanisms of U.S. political oversight can be modified to move toward de-nationalization without threatening the effective operation or freedom of the Internet.

Political Oversight and Public Policy

Political oversight refers to the power of national governments to assert some kind of control over the global Internet. For most governments, this means bringing the Internet into conformity with governmentally established public policies. The WSIS discussions have regularly asserted that governments should be in charge of public policymaking for the Internet.[2]

[1] This paper was written by Milton Mueller with participation from Hans Klein, Jeanette Hofmann, Lee McKnight and Derrick L. Cogburn

[2] The UN Working Group on Internet Governance (WGIG) report, for example, reflected this assumption in tis discussion of "roles and responsibilities" of different actors.Paragraph 30 (page 8) of the WGIG report lists "Public policymaking and coordination and implementation, as appropriate, at the national

There is an important grain of truth in this claim. In national policy making, governments have established institutions for determining the public interest for the national community as a whole. That renders government the most important player in the achievement of societal regulation. Why should the Internet be different?

But there are three fatal problems with national governments as the sole vehicles of public policy making for the Internet. The first is that the Internet is global and states are territorial. The Internet has created an arena for open communication and information exchange across borders. To partition this global space into 200 "sovereign" territories, each with its own laws and regulations, is both practically difficult and potentially crippling of the very freedom to innovate globally that made the Internet a success.

Second, and more fundamentally, a consensus of national *governments* is not a good proxy for the global *public interest*. At the international level, all of the institutional mechanisms for making politicians serve a broader public interest, such as voting, legal checks and balances, lobbying and critical news reporting, are weak or nonexistent. In international politics states are more interested in protecting and extending their own power *as states* than they are in promoting a global public interest.

Third, unless transnational civil society and the business and technical communities are at the table, governments' decisions will be ill-informed at best and positively harmful at worst. A conclave of foreign affairs officials is not capable of understanding, let alone deciding, all global public policy issues related to the Internet. They need the input and participation of other sectors.

For all these reasons, national states should not claim an exclusive role in defining public policy for a global medium such as the Internet. Governments should not be ignored or excluded, but neither should they be pre-eminent. Just as the advent of the railroad elevated governments' economic regulatory capabilities from municipal to provincial and national levels, so the advent of the Internet requires a global approach. And because governments are by nature not global, new arrangements must be made.

Broad and Narrow Oversight

The WSIS debates have combined discussion of two kinds of political oversight: narrow and broad. *Narrow oversight* refers to the policy supervision of ICANN and its administration of Internet identifiers. *Broad oversight* refers to the authority to set global public policy for the Internet on a large range of issues, from intellectual property to spam, interconnection and privacy – policy issues which include but go beyond Internet names and addresses.

Both of these types of political oversight are important. Maintaining a clear distinction between the two, however, can help advance the WSIS negotiations. Today there are no

level, and policy development and coordination at the regional and international levels" as the first "role and responsibility" of governments.

formal mechanisms for broad political oversight of Internet governance. Creating and implementing new institutions for these purposes, assuming that it is desirable, would require sweeping changes and long-term negotiations. ICANN's political oversight, on the other hand, is a more manageable issue and needs to be addressed in the near term. Combining discussion of ICANN's supervision with debates over the governance of all international issues raised by the Internet makes both problems intractable. Each needs to be understood in its own right, and each can be the target of specific policies. Separating debates over the specific issues of ICANN from broader issues of international Internet public policy is a practical step to break the impasse of Prepcom 3.

The rest of this paper concentrates on the narrow oversight issues associated with ICANN. A subsequent paper will discuss steps to address the broader issues.

Current Oversight Mechanisms for ICANN

One of the destructive myths surrounding the current dialogue is that there is currently no political oversight over the Internet. In many countries, but especially the US, the debate on oversight has been framed as a clash between the option of an Internet free from government and an Internet that is "run by the United Nations." That is a false dichotomy, for two reasons. First, it confuses narrow Internet governance (overseeing ICANN) with broader oversight ("running the Internet"). Second, it ignores the fact that political oversight of ICANN exists, but is unilateral: a single government (the US) actively supervises ICANN.

Political oversight of ICANN is conducted using three instruments:

- The ICANN Memorandum of Understanding
- The IANA contract
- The US Cooperative Agreement with VeriSign, Inc.

These contracts are held together by a fourth element:

- A sweeping U.S. assertion of policy authority over the DNS root

Any discussion of the political oversight of ICANN must be grounded in knowledge of these specific mechanisms. They are discussed in detail below.

1. The ICANN Memorandum of Understanding[3]

The U.S. Department of Commerce (DoC) has entered into a Memorandum of Understanding with ICANN, which runs from September 16, 2003 to September 30, 2006. This is the 6th version of the MoU since 1998. The MoU is the primary supervisory document used to control or regulate ICANN conduct. It provides a list of policy making tasks that ICANN is supposed to perform, and sets specific priorities, milestones or accomplishments for ICANN. At present, the MoU's content reflects US policy priorities. It follows the U.S. policy position on new top level domains, privacy in Whois, competition policy, and relations with country code TLD managers. With one-year or

[3] http://www.ntia.doc.gov/ntiahome/domainname/icann.htm

three-year renewal periods since 1998, DoC keeps ICANN on a short leash. Those who assert that the U.S. has a "laissez-faire" policy toward Internet governance probably have never read the MoU. After 2006, the Commerce Department could allow the MoU to expire, setting ICANN free of its oversight. Or it could continue the MoU for yet another defined term. If it continues the MoU, the U.S. could, via negotiations with ICANN, add new tasks or new conditions to it. The MoU is often confused with U.S. policy authority over the DNS root (see #3, below). In fact, it is entirely different. Expiration of the MoU does not necessarily mean the end of U.S. policy authority over the root. Elimination of U.S. policy authority over the root would not necessarily eliminate the MoU.

2. The IANA contract[4]

A zero-price, sole-source contract between ICANN and the US government authorizes ICANN to perform the technical functions of the Internet Assigned Numbers Authority (IANA). This involves administrative activities such as allocating IP address blocks, editing the root zone file, and coordinating the assignment of unique protocol numbers. The IANA contract does not authorize the contractor to change the established policies that guide the performance of the IANA functions. The IANA must rely on ICANN processes to make and change policies (e.g., create a procedure for adding TLDs to the root).

3. "Policy authority" over the DNS root

The U.S. Department of Commerce has since October 1998 asserted what it calls "policy authority" over any and all modifications of the DNS root zone file.[5] When the U.S. first asserted this authority, it was done not to protect the "security and stability of the Internet," but for competition policy reasons. From 1991 to 1998 the root zone file was controlled informally by Jon Postel and its implementation was controlled by Network Solutions, Inc. (predecessor of VeriSign). NSI enjoyed a monopoly on gTLD registrations. The U.S. took over the root in order to facilitate the creation of ICANN and a more competitive market for DNS registrations. During the creation of ICANN the US repeatedly indicated that it would relinquish this authority. Later, and most definitively with the June 30, 2005 "Statement of Principles" by NTIA, it asserted a right to hold on to it forever.[6] This means that USG reserves to itself the authority to approve any changes to the root zone file of the domain name system. In effect, it means that the U.S. owns the root. The U.S. exercises this power not by means of ICANN per se, but through its contract with VeriSign (see #4 below).

[4] The latest version on the web is http://www.icann.org/general/iana-contract-21mar01.htm For an excellent discussion of the nature of this contract in relation to U.S. administrative law, see Michael Froomkin, "Bring on the IANA competitors," ICANN Watch, Feb 3 2003, http://www.icannwatch.org/article.pl?sid=03/02/03/2251256&mode=thread

[5] The assertion of policy authority came in Amendment 11 of the cooperative agreement with Network Solutions, Inc., and takes this form: "While NSI continues to operate the primary root server, it shall request written direction from an authorized USG official before making or rejecting any modifications, additions or deletions to the root zone file."

[6] http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm

4. A cooperative agreement with VeriSign

VeriSign, operator of the .com and .net domains and the world's largest commercial domain name registry, has a cooperative agreement with the U.S. Department of Commerce. The agreement, which dates back to the early days of the public Internet, authorizes it to run the hidden master server that publishes the official root zone file to the Internet's root servers. VeriSign also runs the A root server under this agreement.[7] The agreement is important for two reasons: 1) it was the instrument by which the U.S. government obtained and continues to exercise its authority to control the root[8]; and 2) it compelled VeriSign to conform to the ICANN regime's regulations on registries and registrars.

A Brief Critique of U.S. Unilateralism

The descriptions above reveal an extensive range of oversight functions over Internet names and numbers held exclusively by the United States government. No one should be surprised that this situation has created controversy.

The arguments against perpetuating the current system of unilateral control are legion. The Internet is global, not national. Its value is created by the participation and cooperation of people all over the world. U.S. control of the root has only existed for 7 years, about half of the period of the Internet's public growth and commercialization. While U.S.-based computer scientists invented the TCP/IP protocols long ago, usage and administration of them has become global, and U.S. users are now in the minority. The possession of an exclusive oversight authority by one government, therefore, lacks legitimacy and creates ongoing political conflict and risks of fragmentation.

It is inconsistent for the US to warn of "government intervention" in the Internet while reserving to its own national government special and exclusive powers. The U.S. role is a provocation to other governments, encouraging them to seek equal sovereign rights in the oversight of ICANN. That tension among governments is de-stabilizing. It has already produced several years of increasing politicization of ICANN and its functions. Already, alternative root server systems such as ORSN in Europe have formed to provide a check on U.S. authority over the root zone.

It is a myth that US oversight is a completely neutral and intrinsically harmless. US oversight adds nothing to the technical security of the system and yet presents major opportunities for misuse. The power wielded is not transparent. Negotiations with ICANN and VeriSign over their respective agreements are private. The Commerce

[7] "NSI agrees to continue to function as the administrator for the primary root server for the root server system and as a root zone administrator until such time as the USG instructs NSI in writing to transfer either or both of these functions to NewCo or a specified alternate entity." Amendment 11, DoC-NSI cooperative agreement, October 6, 1998.

[8] Under Amendment 11 of this agreement (October 1998), VeriSign agreed not to modify the root zone file without approval of the US government. The U.S. government did not have any formal authority over the content of the root zone file until this amendment was agreed by VeriSign (called Network Solutions.Inc. at that time). VeriSign was pressured to give up this authority in order to shield itself from an antitrust lawsuit by Name.Space Inc. attempting to add new TLDs to the root.

Department's decisions to include or exclude anything from the MoU follow no process and are bound by nothing but U.S. executive branch policy objectives at the time. And make no mistake about it: the content of the MoU *does* reflect U.S. policy objectives on critical issues such as privacy, competition and intellectual property. The U.S. has even engaged in content regulation. Prodded by lobbying from domestic religious groups close to the Bush administration, DoC intervened in ICANN to delay the creation of a .xxx top level domain for adult content. On questions such as security and surveillance, any U.S. claims of neutrality lack credibility, because it would be impossible for the U.S. not to take its own special interests into account. Finally, the ICANN regime clearly favors U.S.-based economic interests. The redelegation of .org to the Internet Society and the redelegation of .net to VeriSign are the most obvious examples. ICANN tends to move extremely slowly on any changes that would open up the DNS to nonwestern newcomers, such as multilingual top level domains.

Is Change Possible?

Let us now review each of the current oversight mechanisms and discuss the possibilities for change.

Changing the ICANN MoU

It would be relatively easy for the U.S. to change the ICANN MoU. In fact, the contents of the MoU have been amended substantially every time it has been renewed – six times in total. It might be possible, based on agreements coming out of WSIS, for the US to agree to add new items to the MoU reflecting international policy consensus. Or it could take steps to regularize and internationalize the MoU process, e.g. by issuing international requests for comment (RFCs), accepting responses from governments, business and civil society, and then modifying the MoU accordingly (based on a perceived rough consensus and perhaps political considerations). This RFC could be accompanied by a process of global dialogue to collect feedback and ideas on the MoU.

Another possibility is that the USG could simply let the ICANN MoU expire when certain conditions were met. This would allow ICANN to operate with less external supervision. The U.S. would still exercise authority over modification of the root zone file, but policy priorities and outcomes would be directed more by ICANN's own self-governance procedures. Privatization and internationalization of DNS management were the original goals of US policy. The Commerce Department has stated that it would let the MoU expire when it felt that ICANN had achieved maturity as an organization and a suitable record of accomplishment. ICANN itself would support this change. Expiration of the MoU might increase its international legitimacy and would remove a form of oversight that makes its life more difficult. VeriSign might not like this change but would have a difficult time mustering much political support for its position in the U.S. if both the Commerce Department and ICANN supported it.

Changing the IANA contract

In practical terms, it is perfectly feasible to separate the IANA functions from ICANN. Indeed, over the years many parties have complained about the inefficiency of ICANN in performing the IANA functions and have encouraged the US to contract with someone else. But without direct control of the IANA functions, ICANN would lose or weaken its status as the site where policy making processes regarding names and numbers are made. If the IANA functions were shifted to another organization, it would have to agree to passively accept and implement all ICANN decisions, otherwise ICANN's policy making role would become meaningless. Without such an agreement, most participants would abandon ICANN, leaving it without power and financing. Even if a new IANA did agree to implement all ICANN policies, ICANN's influence would be indirect and its power over the Internet would be diminished. As the primary supporter of ICANN, the U.S. government does not want to separate the ICANN and IANA functions. That is why the U.S. government stretches its own laws in order to offer the IANA contract as a noncompetitive, sole source contract. But it is not impossible for the U.S. to open up the IANA contract to competition as long as it retains contractual control over the IANA function. No known U.S. policy statements preclude this.

Change the US Policy Authority over the Root

The U.S. government has made it clear that it does not want to give up its policy authority over the DNS root. It has done so even though the WGIG report identified it as a problem and many other governments, including the European Union, have indicated that they are uncomfortable with the situation. The U.S. claims that its policy authority is required to protect "Internet stability and security." But this is transparently political rhetoric, for everyone wants to maintain the "stability" of the Internet. U.S. oversight as such contributes nothing to the technical security and stability of the DNS; real security comes from the distributed nature of the DNS, the independence and technical expertise of the root server operators, and technical standards implementations such as DNSSEC. Nevertheless, the Bush administration recently obtained bipartisan letters of support from Congress for its position. Among Western business interests, there is a feeling that giving up unilateral control might create political risks by ceding control to unpredictable international political processes. Changing U.S. authority may involve legal as well as political problems. The Executive branch of government may not be able to give up policy authority without congressional authorization. Congressional approval could only come from a highly political process subject to special interest lobbying. International voices would not be represented in this process, only U.S. interests. VeriSign also can be expected to oppose any change here, because it is politically much more influential within a U.S. political environment than in the global one, and its economic prominence in the domain name industry might be more vulnerable if oversight were internationalized. This combination of political and legal forces makes it very difficult to effect immediate change in this area.

Change the VeriSign Cooperative Agreement

The cooperative agreement with VeriSign can also be changed, and has been changed frequently. As a government contract between the U.S. and a private, U.S.-based company, however, it can and probably must reflect domestic policy and very narrow domestic interest calculations. It has always been an objective of US policy to transition the key coordinating functions from the dominant private business that once controlled the root (VeriSign) to ICANN, its chosen nonprofit governance authority. The recent (October 24, 2005) agreement between ICANN and VeriSign starts to move administration of the root zone in that direction, as a quid pro quo for giving VeriSign .net and perpetual control of .com.[9] This shows how the major vested interests involved in the execution of US policy authority over the root (USG, ICANN and VeriSign) reinforce one another's control. Indeed, their propensity to work together has probably been strengthened by the threat of WSIS. While change can happen in this arrangement, it is unlikely to be motivated by external pressures.

In sum, three of the four instruments – the U.S. assertion of policy authority, the IANA contract, and the VeriSign cooperative agreement – constitute a tightly-knit, interdependent set of contractual arrangements that will be difficult to dislodge without major changes in political forces. The MoU on the other hand is a flexible and easily amendable document, and could even be allowed to expire.

The Way Forward

The analysis above has shown that if there are to be any immediate changes the nexus of change must be the ICANN MoU. The process of drafting and amending it offers the best focal point for changing the *status quo*. If we concentrate on the MoU, two basic options present themselves. They are to:

1) Push the ICANN MoU into a more internationalized process
2) Prepare to End the MoU in order to reduce unilateral U.S. oversight.

These two options are often called "**status quo plus**" (#1) and "**status quo minus**" (#2).

Internationalizing the MoU

Since no viable mechanisms for internationalized oversight of ICANN currently exist; political oversight of ICANN must rely on the MoU. The MoU could incorporate international input, in various degrees. At one extreme, one could make its content the basis of negotiation among multiple governments. At the other end of the spectrum, one could formalize a process by which international actors, not only governments but also civil society and business, offered recommendations to the US regarding how to alter the MoU. Either way, international attention should focus on the September 2006 expiration of the current MoU, and begin building recommendations about how the MoU should be modified.

The WGIG Report proposed the creation of a new Multi-stakeholder Forum to discuss global policies. This would be a lightweight discussion forum with equal participation by all parties focused on global Internet policy issues. Numerous commentators have argued convincingly that without a focused purpose, the proposed Forum might be perceived as irrelevant and fail to attract participation and support. One immediate purpose for this new Forum might be to develop policy guidelines to incorporate into the new MoU, which would be offered to the U.S. as non-binding recommendations. Another, less desirable possibility is to modify the MoU to charge ICANN itself with initiating a process to determine a method for internationalizing or privatizing policy authority over

[9] http://www.icann.org/tlds/agreements/verisign/proposed-agreements.htm

the root, just as the 2003 MoU asked ICANN to develop a strategy and policy for adding new top-level domains.

Expiration of the MoU: Reliance on Multistakeholder Governance in ICANN

Another way to deal with the problem of US unilateral oversight is to eliminate as much as possible of the special U.S. role. This approach challenges the need for political oversight by governments. It asserts that a properly constructed ICANN, incorporating input from all stakeholders as equal partners, is sufficient to manage Internet identifiers, including public policy functions.

This option also offers a range of implementation options. The simplest and most extreme is simply for the U.S. to let the MoU expire in 2006, declare ICANN "finished" and walk away. Almost no one, except perhaps for ICANN's management, wants this to happen. There are too many biases and irregularities in the way ICANN is set up. And the U.S. would still retain policy authority over root zone file modification and the IANA contracts. A more intelligent way forward is for the U.S. government, in active consultation with all international stakeholders, to insert a set of conditions into ICANN's MoU that would prepare it for release from U.S. oversight. Once the new conditions of the MoU were met, the MoU would be allowed to expire and would not be replaced with any specific governmental oversight organization. Accountability would rely instead on applicable law and on improvements in process and representation within the broader ICANN regime. This position corresponds roughly to Option 2 of the WGIG Report. A more elaborated and carefully considered development of this idea has come from the WSIS Civil Society Internet Governance Caucus (IGC). We paraphrase below the IGC-proposed conditions for the expiration of the MoU:

- ICANN must ensure full and equal multi-stakeholder participation on its Board
- ICANN must ensure that it establishes clear, transparent, predictable rules and procedures for administrative decision-making
- ICANN must be subjected to independent auditing of its finances
- A process for extraordinary appeal of ICANN'S decisions should be created
- ICANN must negotiate an appropriate host country agreement that releases it from inappropriate national policies of the U.S.
- ICANN's decisions, and any host country agreement, must be required to comply with public policy requirements negotiated through international treaties in regard to, *inter alia*, human rights treaties, privacy rights, gender agreements and trade rules.

Expiration of the MoU under these conditions would not eliminate U.S. policy authority over the root. Our objections to U.S. policy authority remain. But the changes recommended above would de-nationalize the most "political" part of the U.S. political oversight. Once it was no longer combined with the power to guide and direct ICANN's policies and management, U.S. policy authority over the root could become less important.

Analysis of the Options

Option 1: MoU is Internationalized (Status quo plus)

The benefits and risks of this option depend on the specific methods used to insert international input into the MoU. As we noted earlier, agreements among collections of national governments do not necessarily reflect the global public interest. Widespread tinkering with the MoU by multiple governments with conflicting political interests increases the risk that the administration of Internet naming and numbering will be overloaded with intrusive, contradictory and inefficient policy directions. Many of the governments are interested in promoting national sovereignty, which often translates into more control and regulation of the global Internet. On the other hand, if this method relied on the new Multistakeholder Forum proposed by the WGIG Report to develop recommendations, it could avoid many of the risks of too much top-down governmental regulation. But multistakeholderism can easily fail to reach consensus, and could also produce a welter of difficult to implement demands. And long term, this option would still rely on the U.S. government to directly implement and supervise the MoU.

Option 2: MoU Expires (Status Quo Minus)

Option 2 minimizes the threat of centralized governmental control over the Internet; of all the options, it is most likely to keep name and number administration free of destructive intergovernmental politics. Option 2 is probably more politically acceptable to the USG and private sector interests than the other option because of this. If ICANN was suitably reformed prior to its release from the MoU – a big if – this option would preserve and enhance multi-stakeholderism in governance of Internet identifiers. There are, however, negative aspects or risks of this proposal. Insofar as this option requires improvements in ICANN's own internal processes and representation procedures as a quid pro quo, it will be contentious. Who will monitor and enforce these requirements? Who will decide when the conditions have been met? If this is not done properly the process could lead to a bad outcome. The current biases and distortions of ICANN could be rendered permanent. If the proper accountability mechanisms are not in place, ICANN's fees and regulatory authority over the domain name industry could be abused. Prior attempts to subject ICANN to a self-defined independent review process have been abject failures. And regardless of how well the transition goes, some governments may never accept a privatized ICANN as legitimate. These concerns must be taken seriously.

Conclusion

Neither option is perfect. But we do not have the luxury of starting with a blank slate. On the whole, Option 2 appears to be the more politically feasible and desirable path, provided that *serious* reforms in ICANN are made. This requires in particular a host country agreement, and reform of ICANN's Board nomination process, audit/appeal mechanisms, and working methods. With either option, greater use of information and communication technologies and collaboration tools to facilitate geographically distributed participation in deliberation and decision-making is critical.

Most of the objections to WSIS-inspired changes in Internet governance have been grounded in fears about top-heavy governmental meddling in Internet identifier policies, or concerns about the slow and restrictive nature of governmental processes. Governments themselves have generally agreed that they should not be involved in the day to day technical details of managing the Internet. Because it is difficult to extract public policy from the technical details of domain name and IP address administration, it is best to leave identifier policy to a multistakeholder process that captures the expertise and direct involvement of business, the technical community and civil society. It is important to remember that the goal of narrow political oversight is accountability to the *global community of Internet users and suppliers*, not subjection to governments *per se*. Improving ICANN and eliminating unilateral oversight is therefore the more logical path toward reform of political oversight than multilateral involvement of governments.