The World Summit on the Information Society and the Future of Internet Governance

by
*Travis D. Shahan**

I. INTRODUCTION

The final meeting of the World Summit on the Information Society (WSIS), which concluded in November 2005,[1] was built up to be a showdown over the future of Internet governance.[2] When the dust cleared, the issue of Internet governance was still far from settled. For the most part, the delegates to the WSIS agreed to maintain the status quo for the time being, but they also agreed to a mechanism for continuing the Internet governance debate in the future.[3] This paper will analyze the most notable agreements of the WSIS and their effects on the future of Internet governance.

II. DEFINING "INTERNET GOVERNANCE"

One obstacle in the debate over Internet governance is finding a common understanding of the term "Internet governance."[4] In response to a mandate from the WSIS (Phase I), the Working Group on Internet Governance (WGIG) created the following working definition: "Internet governance is the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[5] Under this definition, traditional governments, private indus-

---

* The author is a candidate for Juris Doctor, class of 2007, at Southern Methodist University Dedman School of Law. He earned a Bachelor of Business Administration and a Bachelor of Arts from the University of Oklahoma. He would like to express his sincerest appreciation to his wife, Katie, and son, Luke, for their endless patience and support.

1. World Summit on the Information Society, Basic Information About WSIS: Overview, http://www.itu.int/wsis/basic/about.html (last visited Jan. 15, 2007).

2. *See* Kieren McCarthy, *So Where Are We Up to with This Internet Governance Thing?*, THE REGISTER, Nov. 14, 2005, http://www.theregister.co.uk/2005/11/14/net_governance_wsis/ [hereinafter McCarthy, *So Where Are We?*].

3. Vipin V. Nair, *ICANN to Continue Overseeing the Internet: US Retains Sway; Governance Forum Set Up*, THE HINDU BUSINESS LINE, Nov. 17, 2005, 2005 WL 18565769, *available at* http://www.thehindubusinessline.com/bline/2005/11/17/stories/2005111703130400.htm.

4. *See* Working Group on Internet Governance, Report of the Working Group on Internet Governance ¶ 8 (2005), http://www.wgig.org/docs/WGIGREPORT.pdf.

5. *Id.* ¶¶ 8, 10.

try, and civil society (meaning non-governmental organizations and the general public)[6] all play a role in Internet governance.

The role of governments is one of the most controversial issues in the Internet governance debate. During the early years, when the Internet started to gain widespread use, some users advocated keeping the Internet in the cyberspace equivalent of a state of nature, free from the interference and political oversight of traditional governments.[7] Former Grateful Dead songwriter John Perry Barlow expressed such sentiment in his 1996 *Declaration of the Independence of Cyberspace*.[8] He wrote, "Governments of the Industrial World . . . are not welcome among us."[9] Barlow also proclaimed, "I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us."[10] Contrary to Barlow's vision, traditional governments do in fact influence the Internet. Today, the United States holds more influence over the Internet than any other government due to its authority over the Domain Name System (DNS) and the entities that oversee the DNS, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, Inc. (VeriSign).[11] Just as men in a state of nature might enter into social contracts to gain governmental protection, as Internet conflicts arose, some users entered into agreements that ultimately led to the emergence of ICANN.[12]

The WGIG's working definition of Internet governance purposely covered a broad variety of subjects.[13] The WGIG wanted to make this wide scope evident in its definition:

> Internet governance includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN): it also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet.[14]

---

6. Dick Kaser, *WSIS: Internet Governance Forum Endorsed by World Leaders*, INFORMATION TODAY, INC., Nov. 21, 2005, http://www.infotoday.com/newsbreaks/nb051121-1.shtml.

7. John Palfrey, The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed, 17 HARV. J.L. & TECH. 409, 429 (2004).

8. *Id*.

9. *Id*.

10. *Id*.

11. See Markus Muller, Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 709, 713, 717-18 (2005).

12. *See* Palfrey, *supra* note 7, at 430.

13. *See* Working Group on Internet Governance, *supra* note 4, ¶ 12.

14. *Id*.

But in an effort to refine the debate over the involvement of traditional governments in Internet governance, a group called the Internet Governance Project (IGP) has advocated making a distinction between two types of political oversight over the Internet: narrow oversight and broad oversight.[15] In using the term "narrow oversight," the IGP is referring only to the political oversight of ICANN and the way it affects the DNS.[16] On the other hand, "broad oversight" encompasses political oversight of global public policy on wide-ranging issues—such as spam, privacy, and security—that are far beyond ICANN's scope.[17]

The discussion over the future of Internet governance can be confusing when both narrow and broad oversight are debated without distinction.[18] This paper will focus on the role of traditional governments in Internet governance and examine how the most notable WSIS agreements affect the United States' narrow oversight of the DNS.

III. Internet Basics

In order to understand how the United States has such narrow political oversight over the Internet, it is important to consider some basics of how the Internet works.[19] The Internet has been described as a network of networks.[20] These subnetworks number around 500,000.[21] In order for computers to find each other and communicate in this vast array of networks, each computer connected to the Internet has its own Internet Protocol (IP) address.[22] IP addresses are thirty-two bit numbers expressed in dotted decimal notation.[23] For example, 129.119.70.151 is the IP address for Southern Methodist University's e-mail system. An Internet user can type this number in the address bar of an Internet browser and be directed to Southern Methodist University's website for checking SMU e-mail accounts.[24] The Domain Name System provides a much easier way to access websites. The DNS links IP addresses with domain names, which are much easier to remember.[25]

15. Milton Mueller et al., Internet Governance Project, Political Oversight of ICANN: A Briefing for the WSIS Summit 2 (2005), http://www.internetgovernance.org/pdf/political-oversight.pdf.
16. *See id.*
17. *See id.*
18. *See id.* at 3.
19. *See* Muller, *supra* note 11, at 713.
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. Last attempted Jan. 15, 2007.
25. Muller, *supra* note 11, at 714.

For example, instead of having to remember the exact Southern Methodist University IP address, users can reach the same website by typing in its domain name, "webmail.smu.edu." When a user searches for a particular domain name, the DNS finds the IP address for the desired domain name and facilitates the connection between the user's computer and the computer the user is seeking to reach.[26] Because of the DNS, users do not have to remember long numeric IP addresses.[27]

Domain names contain different parts.[28] The section furthest to the right of each domain name—for example, the ".edu" in "webmail.smu.edu"—identifies the top-level domain (TLD) to which the domain name belongs.[29] The DNS has a restricted number of TLDs. TLDs like ".com," ".edu," and ".net," are examples of generic TLDs (gTLDs), of which there are only fourteen altogether.[30] There are also 249 two-letter country-code TLDs (ccTLDs) such as ".ca" for Canada, ".mx" for Mexico, and ".us" for the United States.[31] The next to the last part of each domain name—for example, the ".smu" in "webmail.smu.edu"—is called the second-level domain.[32] This naming system can be thought of as a tree-like hierarchy.[33] Each TLD has numerous second-level domains that can have third-level domains—for example, the "webmail" in "webmail.smu.edu"—and so on.[34]

The most important parts of the DNS are the root zone file and name servers.[35] The root zone file is like a master list of all TLDs and the name servers to which each TLD has been assigned.[36] The original, authoritative root zone file is kept on the "A-root-server," which the company VeriSign operates in Virginia.[37] In turn, each name server keeps track of all the second-level domains of the TLD assigned to it.[38] The name servers store the

26. *See id.*

27. *Id.*

28. *See id.*

29. *Id.*

30. *See* ICANN, Top-Level Domains (gTLDs), http://www.icann.org/tlds/ (last visited Jan. 15, 2007) (explaining that the fourteen gTLDs are .com, .edu, .gov, .int, .mil, .net, .org, .biz, .info, .name, .pro, .aero, .coop, and .museum); *see also* Muller, *supra* note 11, at 714.

31. *See* IANA, Root-Zone Whois Information, Index by TLD Code, http://www.iana.org/cctld/cctld-whois.htm (last visited Jan. 15, 2007).

32. Muller, *supra* note 11, at 714.

33. ICANN, Top-Level Domains (gTLDs), *supra* note 29.

34. *Id.*

35. *See* Muller, *supra* note 11, at 714.

36. *See id.* at 714-15.

37. *Id.* at 715.

38. *See id.*

matching IP addresses for the second-level domains of the particular TLDs they are assigned.[39] The root zone file is the heart of the DNS because, "[b]y referring to a particular name server, the root file gives that name server control over the domain names in that TLD."[40] The root zone file informs Internet users which name servers are authoritative for a given TLD.[41]

Altogether, there are thirteen root servers to help relieve congestion.[42] These servers are identified by the letters A through M.[43] The A-root-server maintains the authoritative copy of the root zone file, which is then made available to the twelve other root servers.[44] In addition to the main A-root-server, VeriSign also manages the J-root-server.[45] Other root server operators include the National Aeronautics and Space Administration (NASA), two U.S. military agencies, and ICANN.[46] The rest of the root server operators are private entities.[47] Ten of the thirteen root servers are located in the United States.[48] The remaining three are located in the United Kingdom, Japan, and Sweden.[49]

The physical channels conveying data over the Internet are the "backbone" and the "local loop."[50] The backbone is a collection of large conduits connecting Internet Service Providers (ISPs) with each other.[51] The local loop refers to the smaller connections linking individual users with their chosen ISPs.[52] The entities physically controlling the backbone and local loop in any given area have the power to filter the information available on these channels.[53] Thus, if a particular government controls the backbone and local

39. *See id.*

40. *Id.*

41. Kim G. von Arx & Gregory R. Hagen, *A Declaration of Independence of ccTLDs from Foreign Control*, 9 RICH. J.L. & TECH. 1, 2 (2002).

42. Harold Feld, *Structured to Fail: ICANN and the "Privatization" Experiment*, *in* WHO RULES THE NET? 333, 337 (Adam Thierer & Clyde Wayne Crews Jr. eds., 2003).

43. von Arx & Hagen, *supra* note 40, at 15.

44. *Id.*

45. VeriSign, Corporate Overview, Fact Sheet, http://www.verisign.com/verisign-inc/corporate-overview/fact-sheet/index.html (last visited Jan. 15, 2007).

46. Feld, *supra* note 41, at 337.

47. *Id.*

48. von Arx & Hagen, *supra* note 40, at 16.

49. *Id.* at 15.

50. Muller, *supra* note 11, at 723.

51. *Id.*

52. *See id.*

53. *See id.*

loop within its territory, that government can censor certain information and exert great control over the content its citizens may access.[54]

IV. Evolution of Domain Name System Internet Governance

The United States' historic role in helping develop the Internet has given it much influence over the DNS and root zone file. This influence arose because the funding to develop the DNS came from grants from the U.S. government.[55] The DNS was developed in 1983 by scientists such as Jon Postel and Paul Mockapetris.[56] While a graduate student at UCLA, Postel received funding from the U.S. Department of Defense (DoD) and assumed responsibility for the informal coordination of a number of Internet activities, including assigning IP numbers and deciding which gTLDs and ccTLDs would be created.[57] After he received his doctoral degree, Postel continued to spearhead these functions, relocating his operation to the University of Southern California's Information Sciences Institute (ISI).[58] Eventually, ISI reorganized and, under the leadership of Postel and with authority from the DoD, began operating administrative aspects of the DNS as the Internet Assigned Numbers Authority (IANA).[59] IANA was the government contractor responsible for "the allocation and assignment of various identifiers needed for the operation of the Internet."[60] These administrative functions, such as "allocating IP address blocks, editing the root zone file, and coordinating the assignment of unique protocol numbers," became known as the IANA functions.[61]

While Postel and IANA took the lead in shaping DNS policy, operational control of the root zone file was handled by others who were also originally funded by the DoD.[62] In the early 1990s, the DoD contracted with Government Systems Inc. (GSI), which then subcontracted with Network Solutions, Inc. (NSI) to operate the root zone file.[63] In 1993, the National Science Foundation (NSF) assumed the DoD's role in funding this contract.[64]

54. *See id.*

55. A. Michael Froomkin, Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, 50 Duke L.J. 17, 51 (2000).

56. Peter K. Yu, *The Origins of ccTLD Policymaking*, 12 Cardozo J. Int'l & Comp. L. 387, 390 (2004).

57. Froomkin, *supra* note 54, at 52-53.

58. *Id.* at 53.

59. *Id.*

60. *Id.* at 53 n.121, 54.

61. *See* Mueller et al., *supra* note 15, at 4.

62. *See* Froomkin, *supra* note 54, at 52.

63. *See id.* at 55.

64. *Id.* at 57.

Under this agreement between NSF and NSI, NSI handled more than just the root zone file.[65] NSI "ran the computers that held the root zone, was responsible for the mechanics of inserting new TLDs into the root (although not for deciding which, if any, should be included), and also took on the function of day-to-day assignment of second-level domain names in .com, .org, and .net."[66] This agreement gave NSI a monopoly over registrations in these gTLDs that was set to expire in 1998.[67] Finally, the NSF-NSI agreement required NSI to follow policy as set by IANA, which was still funded by the DoD.[68] Subsequently, NSF transferred its role in the agreement to the National Telecommunications and Information Administration at the U.S. Department of Commerce (DoC).[69] Therefore, until 1998, Postel and IANA set standards for administering the DNS that were then implemented by NSI.[70]

Since 1998, the organization responsible for the management of the DNS has been the Internet Corporation for Assigned Names and Numbers.[71] ICANN was officially established on September 30, 1998, as a nonprofit organization incorporated in and operating out of California.[72] "ICANN emerged from a U.S. government initiative, in concert with members of the private sector and the technical Internet community, intending to resolve the brewing dispute over governance of the DNS."[73] As the Internet grew and disputes over the DNS emerged, management of the DNS became too much for IANA alone.[74] The United States government did not want to take over management of the DNS.[75] Instead, the U.S. decided private sector management would result in a better system.[76] ICANN turned out to be the vehicle for attempting this privatization.

The United States government supported ICANN's assumption of this role from the beginning.[77] It expected Postel to be heavily involved with ICANN.[78] Postel incorporated ICANN and was set to serve as its chief tech-

65. *See id*.

66. *Id*.

67. *Id*; MUELLER ET AL., *supra* note 15, at 4.

68. Froomkin, *supra* note 54, at 57-58.

69. Feld, *supra* note 41, at 346.

70. *See* MUELLER ET AL., *supra* note 15, at 4.

71. *See* Palfrey, *supra* note 7, at 421.

72. *Id*. at 427.

73. *Id*. at 420.

74. *Id*. at 419.

75. *See id*. at 420.

76. *See id*.

77. *See* Froomkin, *supra* note 54, at 70.

78. *See id*.

nical officer.[79] Furthermore, it is believed that he played a large role in selecting ICANN's first officers and board of directors.[80] According to Professor A. Michael Froomkin, the DoC wanted "to find a more formal structure for DNS management that left it in Postel's capable hands—and could be presented as a pro-Internet, deregulatory victory for the Clinton administration."[81] Froomkin also maintains, "ICANN exists because the Department of Commerce called for it to exist."[82] Postel's involvement with ICANN ended prematurely, though, due to his sudden death on October 16, 1998, just as ICANN was starting out.[83]

On October 7, 1998, the United States and NSI amended their agreement concerning operation of the root zone file.[84] Significantly, under this new agreement, NSI continued operation of the root zone file, but any decisions on possible additions or deletions to the file now had to be approved in writing by the DoC.[85] NSI also agreed to allow competing registrars to sell domain name registrations, which set the stage for the separation of NSI's registry and registrar functions.[86] NSI assented to this agreement in part to shield itself from antitrust litigation by Name.Space Inc., a company that sought to add new TLDs to the root.[87] Nevertheless, the agreement remained favorable to NSI because as a registry operator, it could charge a fixed fee to new registrars that entered the market.[88] In fact, NSI's continued power to assign and manage particular domain name registry systems made it so valuable that in 2000, VeriSign purchased NSI for $21 billion.[89]

On November 25, 1998, the DoC and ICANN entered into a Memorandum of Understanding (MoU).[90] The MoU is an important part of ICANN's authority.[91] Professor Froomkin gives the following analysis of the MoU:

> On its face, the document conveys no direct authority, only the power to make a study of how the DNS would be privatized in the future. In fact, however, the DoC-ICANN MoU conveyed very

79. *Id*. at 72.

80. Palfrey, *supra* note 7, at 420.

81. Froomkin, *supra* note 54, at 70.

82. *Id*.

83. *Id*. at 73.

84. *Id*. at 81.

85. *See id*.

86. *Id*.

87. MUELLER ET AL., *supra* note 15, at 5 n.8.

88. *See* Froomkin, *supra* note 54, at 81.

89. Palfrey, *supra* note 7, at 434.

90. Froomkin, *supra* note 54, at 84.

91. *See id*.

> significant authority, because the means by which ICANN would "study" the future privatization of the DNS was by acting as if the DNS were already privatized.[92]

Included in this agreement were such goals as:

> [E]ncouraging international participation, providing expertise and advice on the allocation of IP number blocks and coordinating the assignment of other Internet technical parameters as needed to maintain universal connectivity of the Internet, collaborating on written technical parameters for operation of the authoritative root, and collaborating on a study and process to address operational requirements of the root name servers and the security of the root server system.[93]

Separate from the MoU, the DoC and ICANN needed a different agreement to formalize ICANN's authority over the technical aspects of the DNS.[94] In June 1999, the U.S. government contracted to give ICANN the responsibility for the IANA functions.[95] This zero-price, sole source contract made ICANN responsible for administrative activities including: the allocation of IP address blocks, the editing of the root zone file, and the assignment of unique protocol numbers.[96] The IANA contract did not grant authority to make or change policy, but merely granted ICANN the authority to handle the technical IANA functions.[97] Prior to this agreement with the DoC, ICANN had already seemingly enveloped the IANA organization.[98] ICANN maintained its headquarters in Marina Del Rey, California, in the same office building that served as headquarters for IANA.[99] In addition, ICANN and the University of Southern California reached an agreement under which ICANN received IANA assets and personnel and assumed IANA's liabilities.[100] The June 1999 agreement made ICANN's assumption of the IANA functions official.

---

92. *Id*.

93. Palfrey, *supra* note 7, at 421-22.

94. *See* Froomkin, *supra* note 54, at 85.

95. *Id*. at 85-86.

96. MUELLER ET AL., *supra* note 15, at 4.

97. *Id*.

98. *See* Froomkin, *supra* note 54, at 85-86.

99. *Id*. at 85.

100. *Id*. at 86.

V. Why the United States Has so Much Influence

The United States exercises narrow oversight of ICANN and the DNS with a series of contracts.[101] The most important contracts are the root zone file agreement with VeriSign, the ICANN Memorandum of Understanding, and the contract granting ICANN the IANA functions.[102] These contracts are the means by which the United States exerts limited control over the Internet.

A. Root Zone File Agreement Between the U.S. and VeriSign

Since October 1998, the United States has asserted "policy authority" over any changes to the root zone file.[103] Control over the root zone file means control over the entire DNS, which can translate into significant influence on the Internet as a whole.[104] The root file stored on the A-root-server is followed because it was the first root created.[105] Alternative roots are possible, but they are not likely to be successful due to the confusion they would create, since an alternative root would mean a given domain name might not always lead to the same website.[106] If someone established a network that followed a root file different from the original, other users might avoid connecting to that network in order to maintain consistency.[107]

The United States has influence over the root zone file in two ways. First, the U.S. physically protects the root zone file from interference from other governments since it is located within its borders on the A-root-server in Virginia.[108] Second, and more importantly, VeriSign (successor to NSI) has contractually agreed to make any changes to the root zone file contingent on written approval from the DoC.[109] Until this agreement with NSI, the United States did not have any formal power over the root zone file.[110] The agreement stated specifically, "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."[111] The United States pushed for this veto power in order to advance ICANN's legitimacy, with an eye toward eventually ceding all root

101. *See* Muller, *supra* note 11, at 719.

102. Mueller et al., *supra* note 15, at 3.

103. *Id.* at 4.

104. Muller, *supra* note 11, at 713.

105. *See id.* at 716.

106. *See id.*

107. *See id.*

108. *Id.* at 717.

109. *See id.*

110. Mueller et al., *supra* note 15, at 5 n.8.

111. *Id.* at 4 n.5.

file operations to ICANN.[112] With this important veto power, the U.S. can compel VeriSign to abide by ICANN's regulations.[113]

Soon, in addition to setting standards for the root zone file, ICANN may also gain administrative control of it. "It has always been an objective of [United States] 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."[114] On October 24, 2005, VeriSign and ICANN negotiators reached a litigation settlement agreement that, among other things, could transfer administration of the root zone file to ICANN.[115] In return, VeriSign continues to control the .net domain and essentially has perpetual control of the .com domain.[116] The ICANN Board of Directors approved this agreement on February 28, 2006,[117] and the DoC announced its approval on November 30, 2006.[118]

B. Memorandum of Understanding Between the U.S. and ICANN

The main document the United States relies upon to supervise ICANN is the Memorandum of Understanding.[119] The MoU between ICANN and the DoC also serves as a main source of ICANN's authority.[120] The original MoU was reached when ICANN was formed in 1998.[121] Currently, ICANN operates under the seventh version of the MoU, called the Joint Project Agreement (JPA).[122] The JPA became effective on September 29, 2006, and

112. *See id.* at 4, 7.

113. *See id.* at 5.

114. *Id.* at 7.

115. *See id.* at 7-8.

116. *Id.* at 8.

117. Press Release, ICANN, ICANN Board Approves VeriSign Settlement Agreements (Feb. 28, 2006), http://www.icann.org/announcements/announcement-28feb06.htm.

118. *See* Press Release, Nat'l Telecomms. & Info. Admin., U.S. Dep't of Commerce, NTIA Approves New .Com Registry Agreement (Nov. 30, 2006), http://www.ntia.doc.gov/ntiahome/press/2006/icanncom_113006.pdf.

119. MUELLER ET AL., *supra* note 15, at 3.

120. *See* Palfrey, *supra* note 7, at 421.

121. *See* MUELLER ET AL., *supra* note 15, at 3.

122. *See* Press Release, Nat'l Telecomms. & Info. Admin., U.S. Dep't of Commerce, U.S. Commerce Department Announces a Joint Project Agreement with ICANN on the Coordination of Internet Domain Name and Addressing System (Sept. 29, 2006), http://www.ntia.doc.gov/ntiahome/press/2006/icannmou_09292006.pdf; *cf.* MUELLER ET AL., *supra* note 15, at 3.

is scheduled to run until September 30, 2009.[123] Some have suggested that by limiting the renewal periods to one or three years, the DoC "keeps ICANN on a short leash."[124] Also, this delegation of authority can be revoked at the United States' option by providing 120 days' notice.[125] The MoU provides the United States significant influence over ICANN policy.[126]

C. IANA Contract Between the U.S. and ICANN

The United States also influences the DNS by determining who it contracts with to perform the IANA functions. Technically, the DoC has the power to grant the contract to perform IANA functions to whomever it wishes.[127] This means that ICANN is not guaranteed to win this contract each time it comes up for renewal.[128] ICANN's power would be greatly weakened if the United States were to grant the IANA contract to another organization because it would no longer be able to directly ensure that the policies it adopted were carried out in practice.[129] Since the United States is the main supporter of ICANN, it is not likely to undercut ICANN by granting IANA administration to any other entity.[130] However, this possibility gives the U.S. significant negotiating power with respect to ICANN.

VI. Criticism of Current DNS Management System

Some critics of ICANN question the legitimacy of the organization because its authorization was granted by just one nation, the United States.[131] Others criticize ICANN's legitimacy based on the fact that its corporate structure relies on the laws of just one U.S. state, California.[132] ICANN has also faced accusations that it is not as open or representative as it was intended to be.[133] ICANN's complex organizational form has been described as an accidental hybrid of a corporation, a standards body, and a government

123. Joint Project Agreement Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers 2-3 (2006), http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/signedmou290906.pdf [hereinafter Joint Project Agreement].

124. *Id.* at 3-4.

125. Muller, *supra* note 11, at 718; *see also* Joint Project Agreement, *supra* note 122, at 2.

126. *See* Mueller et al., *supra* note 15, at 3.

127. *See id.* at 7.

128. *See id.*

129. *Id.*

130. *Id.*

131. Palfrey, *supra* note 7, at 419.

132. *Id.* at 427.

133. *Id.* at 437-465.

entity.[134] Some say it is this complexity that hinders transparency and makes broad public participation difficult.[135]

The Internet Governance Project argues that the ways in which the United States influences the Internet are not transparent enough.[136] It points out that U.S. negotiations with both ICANN and VeriSign remain private.[137] The IGP claims that the United States has even gone so far as to regulate content on the Internet by disrupting the creation of the proposed ".xxx" gTLD for adult content.[138] The IGP also criticizes the current system because "ICANN tends to move extremely slowly on any changes that would open up the DNS to nonwestern newcomers, such as multilingual top level domains."[139]

VII. World Summit on the Information Society

At the United Nations Millennium Summit in September 2000, the U.N. set eight major goals to be accomplished by 2015.[140] Collectively, these goals are referred to as the Millennium Development Goals.[141] The last of these goals is to "create a global partnership for development, with targets for aid, trade and debt relief."[142] One aim of this final goal is to cooperate with the private sector in order to "make available the benefits of new technologies—especially information and communications technologies."[143] The United Nations hopes to bridge the "digital divide" between rich and poor countries.[144] The World Summit on the Information Society provided an opportunity for representatives of many nations to discuss in depth how to best achieve this aim.

134. *Id*. at 414-15.

135. *See id*. at 415.

136. Mueller et al., *supra* note 15, at 5.

137. *Id*.

138. *See id*. at 6.

139. *Id*.

140. United Nations, Implementing the Millennium Declaration 1-2 (2002), http://www.un.org/millenniumgoals/MDGs-FACTSHEET1.pdf.

141. *Id*. at 1.

142. *Id*. at 2.

143. The UN Millennium Development Goals, http://www.un.org/millenniumgoals/goals.html (last visited Jan. 15, 2007).

144. World Summit on the Information Society, Basic Information About WSIS: Why a Summit on the Information Society, http://www.itu.int/wsis/basic/why.html (last visited Jan. 15, 2007).

The International Telecommunication Union (ITU), a specialized agency within the United Nations system,[145] was given the lead role in facilitating the WSIS.[146] With Resolution 56/183 in 2001, the United Nations General Assembly endorsed the ITU's plan for the WSIS and gave it the lead role in organizing the summit.[147] The WSIS was held in two phases.[148] The first phase was held in Geneva from December 10 to December 12, 2003, and involved more than 11,000 participants from 175 countries.[149] The second phase took place in Tunis from November 16 to November 18, 2005, with more than 19,000 participants from 174 countries.[150] While U.N. Secretary-General Kofi Annan claimed that "[t]he main objective of the World Summit on the Information Society . . . is to ensure that poor countries get the full benefits that new information and communication technologies—including the Internet—can bring to economic and social development,"[151] the issue that received the most attention and stirred the most controversy was the issue of Internet governance.[152]

A. WSIS Phase I (Geneva)

The main outcome of the Geneva phase of the WSIS was the eventual formation of the Working Group on Internet Governance.[153] Paragraph 13 of the Plan of Action adopted in Geneva made the following request:

> 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 investi-

145. UNITED NATIONS, THE UNITED NATIONS SYSTEM (2004), http://www.un.org/aboutun/unchart.pdf.

146. World Summit on the Information Society, Basic Information About WSIS: Why a Summit on the Information Society, *supra* note 143.

147. *Id.*

148. World Summit on the Information Society, Basic Information About WSIS: Overview, *supra* note 1.

149. *Id.*

150. *Id.*

151. Kofi A. Annan, Letter to the Editor, *The U.N. Isn't a Threat to the Net*, WASH. POST, Nov. 5, 2005, at A19, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/11/04/AR2005110401431_pf.html.

152. See McCarthy, So Where Are We?, supra note 2.

153. *See* Working Group on Internet Governance (WGIG) Home Page, http://www.wgig.org/ (last visited Jan. 15, 2007).

> gate and make proposals for action, as appropriate, on the governance of Internet by 2005.[154]

The WGIG issued its final report in June 2005 so that it could be discussed at the second phase of the WSIS held later that year.[155] The WGIG's final report presented four proposed models for Internet governance change.[156]

WGIG's Model 1 proposed the formation of a Global Internet Council (GIC) "anchored in the United Nations."[157] The GIC would be made up of members from governments.[158] Governments then would play the leading role in this new organization with the private sector and civil society only playing advisory roles.[159] Regarding international Internet governance, the GIC would displace the DoC as well as replace ICANN's Governmental Advisory Committee (GAC).[160] ICANN would then become accountable to the GIC.[161] Most notably, GIC would take over the oversight of "additions or deletions to the root zone file, management of IP addresses, introduction of gTLDs, [and] delegation and redelegation of ccTLDs."[162]

WGIG's Model 2 recommended eliminating the United States' unique oversight of ICANN but, unlike the other models, did not propose that any new entity assume that role. This model claimed, "There is no need for a specific oversight organization,"[163] however, it also acknowledged that "[i]t may be necessary to enhance the role of ICANN's Governmental Advisory Committee (GAC) in order to meet the concerns of some Governments on specific issues."[164] Model2 also reiterated the proposal for the multi-stakeholder forum for global discussion of Internet issues that the WGIG proposed earlier in its report.[165]

---

154. World Summit on the Information Society, Geneva, Switz., Dec. 10-12, 2003, *Plan of Action*, ¶ 13, U.N. Doc. WSIS-03/GENEVA/DOC/5-E (Dec. 12, 2003), *available at* http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf.

155. *See* Working Group on Internet Governance (WGIG) Home Page, *supra* note 152.

156. Working Group on Internet Governance, *supra* note 4, ¶ 37.

157. *Id*. ¶¶ 52, 55.

158. *Id*. ¶ 52.

159. *Id*. ¶ 56.

160. *Id*. ¶ 52.

161. *Id*. ¶ 54.

162. *Id*. ¶ 53.

163. *Id*. ¶ 57.

164. *Id*. ¶ 58.

165. *See id*. ¶¶ 59-61.

The next WGIG proposal, Model 3, envisioned the formation of an International Internet Council (IIC).[166] This model suggested that since "no single Government should have a pre-eminent role in relation to international Internet governance," the IIC could have policy oversight of ICANN, thereby having oversight of the management of the DNS.[167] Model 3 also hinted that ICANN's GAC would no longer be necessary if the IIC had oversight of ICANN.[168] Similar to Model 1, governments would have the leading role in the IIC while the private sector and civil society could only provide advice.[169] Finally, this model called for a "host-country agreement for ICANN."[170]

WGIG's Model 4 was the longest and most radical of the four alternatives. This model proposed a number of new organizations. One proposed new organization was the Global Internet Policy Council (GIPC).[171] The GIPC would be responsible for developing public policy regarding international Internet-related issues.[172] Similar to the GIC proposed in Model 1 and the IIC proposed in Model 3, the GIPC would be government-led; however, the private sector and civil society would be limited to being observers.[173] The most significant changes proposed in Model 4 related to ICANN. While the other models may have proposed changes to ICANN's oversight, Model 4 went much further. Model 4 envisioned the formation of a World Internet Corporation for Assigned Names and Numbers (WICANN), a "reformed internationalized ICANN linked to the United Nations."[174] WICANN would be "[r]esponsible for the 'development of the Internet in both technical and economic fields.'"[175] Though Model 4 claimed that WICANN would be led by the private sector with governments and civil society participating in an "observer/advisory capacity,"[176] this model seems to give governments much more power than that. The model proposed that governments assume both an advisory role and an oversight role.[177] The advisory role could possibly replace the GAC that advises the current ICANN.[178] The oversight role of WICANN would be carried out by yet another organization called the Over-

166. *Id.* ¶ 62.

167. *Id.*

168. *See id.* ¶ 66.

169. *Id.* ¶ 64.

170. *Id.* ¶ 67.

171. *Id.* ¶ 69.

172. *Id.* ¶¶ 68-69.

173. *Id.* ¶ 69.

174. *Id.* ¶ 70.

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.*

sight Committee.[179] The Oversight Committee would be appointed by and report to the proposed GIPC.[180] While the proposed oversight "would not be of an operational or management nature," this committee would replace the oversight currently exercised by the DoC.[181] Also, similar to Model 3, a host-country agreement would be implemented for WICANN.[182] Finally, comparable to Model 2, Model 4 called for the formation of the Global Internet Governance Forum where governments, the private sector, and civil society would play equal roles in discussing Internet-related public policy issues.[183]

B. WSIS Phase II (Tunis)

The Tunis phase of the WSIS shaped up to be a showdown between those wanting to maintain the status quo regarding Internet governance, such as the United States, and those who sought to reduce U.S. influence over the Internet, such as Brazil, China, and Iran.[184] Ultimately, the United States held its ground and did not cave in to the wishes of some other countries that sought to minimize its role in Internet governance. None of the WGIG's four proposed models for a new form of Internet governance was adopted.[185] The delegates agreed to work within the existing Internet governance framework,[186] leaving ICANN's oversight of the Internet undisturbed.[187] While the status quo was preserved for the most part, the concluding phase of the WSIS did produce three notable agreements: recognition that all governments should play a part in Internet governance, agreement on the treatment of ccTLDs, and creation of the new Internet Governance Forum (IGF).

While the United States maintained its ground for the time being, the WSIS did not leave U.S. opponents empty-handed. Paragraph 68 of the Tunis Agenda for the Information Society (Tunis Agenda) stated, "We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and

179. *Id.*

180. *Id.*

181. *Id.*

182. *Id.*

183. *Id.* ¶ 71.

184. See McCarthy, So Where Are We?, supra note 2.

185. Kaser, *supra* note 6.

186. Kieren McCarthy, *US Wins Net Governance Battle*, THE REGISTER, Nov. 16, 2005, http://www.theregister.co.uk/2005/11/16/us_wins_net_governance/ [hereinafter McCarthy, *US Wins Net Governance Battle*].

187. Nair, *supra* note 3.

continuity of the Internet."[188] Opponents of the current DNS management structure are likely to point to this language as support for their calls for change.[189]

Another significant aspect of the Tunis Agenda concerned country-code top-level domains. Under this agreement, the delegates recognized the great interest that national governments have in their own ccTLDs. Specifically, Paragraph 63 of the Tunis Agenda stated, "Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms."[190] This agreement is not as groundbreaking as it might first appear, because ICANN had already decided to treat ccTLDs in a manner consistent with the language in Paragraph 63.[191]

Perhaps the most publicized outcome of the WSIS was the agreement to convene the Internet Governance Forum in 2006. The decision to organize another global forum to continue the discussion of Internet issues resulted from one of the recommendations of the WGIG.[192] This recommendation was adopted and expressed in Paragraphs 72 through 79 of the Tunis Agenda.[193] Paragraph 72 began by asking "the UN Secretary-General, in an open and inclusive process, to convene, by the second quarter of 2006, a meeting of the new forum for multi-stakeholder policy dialogue—called the *Internet Governance Forum* (IGF)."[194] The inaugural meeting of the IGF finally took place in Athens from October 30 to November 2, 2006.[195]

---

188. World Summit on the Information Society, Tunis, Tunis., Nov. 16-18, 2005, *Tunis Agenda for the Information Society*, ¶ 68, U.N. DOC. WSIS-05/TUNIS/DOC/6(Rev.1)-E (Nov. 18, 2005), *available at* http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf [hereinafter *Tunis Agenda*].

189. *See* Victoria Shannon, *Victory Claims Abound for Global Web Accord*, INT'L HERALD TRIB., Nov. 17, 2005, at News3, *available at* 2005 WL 18758064.

190. *Tunis Agenda*, *supra* note 187, ¶ 63.

191. *See* Kaser, *supra* note 6.

192. *Id.*

193. IGFGreece2006.gr, About the Forum, http://www.igfgreece2006.gr/index.php?tid=29&aid=0 (last visited Jan. 15, 2007).

194. *Tunis Agenda*, *supra* note 187, ¶ 72.

195. The Internet Governance Forum (IGF) Home Page, http://www.intgovforum.org (last visited Jan. 15, 2007).

VIII. Analysis of Most Notable WSIS Agreements

A. Analysis of Recognition that All Governments Should Have an Equal Role in Internet Governance

The language in Paragraph 68 of the Tunis Agenda stating that all governments should have an equal role in Internet governance gives ammunition to those calling for the United States to hand what Internet control it has over to an international body.[196] For example, French delegate Bernard Benhamou's statements after the agreement show that opponents of the U.S. will continue to seek concessions. While recognizing that "[t]he oversight is in the U.S. now and for the time being," Benhamou also pointed out, "but now there is a process set in motion to consider alternatives to that."[197] Perhaps most tellingly, when referring to the United States maintaining narrow oversight, Benhamou stated, "They have bought some time."[198]

It is important to recall the Internet Governance Project's distinction between narrow oversight of ICANN and broad oversight of global Internet public policy.[199] When critics of the current Internet governance system call for less involvement on the part of the United States, they often seem to confuse narrow oversight with broad oversight.[200] Those who see less United States involvement as a cure-all fail to recognize that while the United States does have significant influence over the narrow oversight of ICANN and the DNS, it is not a global Internet dictator.

The only power the United States can possibly concede is that which it actually possesses. The United States only has narrow oversight over ICANN, not broad oversight over all Internet public policy.[201] As the IGP points out, "Today there are no formal mechanisms for broad political oversight of Internet governance."[202] ICANN's website explains that its responsibilities are limited to the technical coordination of the DNS:

> ICANN is responsible for coordinating the management of the technical elements of the DNS to ensure universal resolvability so that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique technical identifiers used in the Internet's operations, and delegation of Top-Level Domain names (such as .com, .info, etc.).[203]

196. *See* Shannon, *supra* note 188.

197. *Id.*

198. *Id.*

199. *See* Mueller et al., *supra* note 15, at 2.

200. *See id.* at 3.

201. *See id.*

202. *See id.* at 2-3.

203. ICANN, Welcome to ICANN!, http://www.icann.org/new.html (last visited Jan. 15, 2007).

While other issues such as spam, Internet security, etc. are important to Internet users worldwide, these issues are beyond ICANN's scope.[204]

Fears of a U.S. monopoly on broad oversight of the Internet are unfounded, but what about calls for the United States to relinquish some of its narrow oversight? Due to its historic role in fostering the development of the Internet and the DNS, ultimately, the United States alone has complete narrow oversight. Other governments do have a voice, though, through ICANN's Governmental Advisory Committee.

The GAC was formed with the purpose of providing an organization where the world's nearly 200 governments could come together to discuss policies affecting the Internet and the DNS.[205] According to ICANN's bylaws, representatives of national governments, multinational governmental organizations, and treaty organizations can all be members of the GAC.[206] Yet, any decision it makes is non-binding on ICANN because the GAC only provides advice.[207] Even so, the President and CEO of ICANN, Dr. Paul Twomey, pointed out that while decisions of the GAC must be approved by the ICANN Board of Directors in order to go into effect, the Board has always followed the GAC's decisions.[208]

While all the governments of the world are welcome to participate in the GAC, those participating regularly number no more than about thirty.[209] Some of the loudest critics of the United States and ICANN, such as Brazil, China, and Russia, have for the most part ignored participating in the GAC process.[210]

The calls for the United States to concede narrow oversight of ICANN and the DNS to an international governmental body are unwarranted. Other governments of the world already have a say in the operation of the DNS through the GAC.[211] Obviously ICANN is responsive to concerns of governments if it has yet to disagree with a GAC decision.[212] Criticism from governments that have chosen not to even participate in the GAC should not be given any weight. It is not the United States' fault that these countries prefer to complain from the sidelines rather than address their concerns and take

204. *Id*.

205. 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, 1115 (2003).

206. *Id*.

207. *See id*.

208. McCarthy, US Wins Net Governance Battle, supra note 185.

209. Kleinwoechter, *supra* note 204, at 1116.

210. *Id*.

211. *See* McCarthy, *US Wins Net Governance Battle*, *supra* note 185.

212. See id.

positive steps to effect change through the body established for that specific purpose.

The hypocrisy of some critics is extraordinary. One example can be found in the post-WSIS statements of the Secretary-General of the International Telecommunication Union, Yoshio Utsumi. In September 2005, prior to the Tunis phase of the WSIS, Utsumi stirred up quite a controversy when he claimed that the ITU was prepared to take over the running of the Internet.[213] This assertion helped galvanize the lobbying efforts of those who feared U.N. control of the Internet, which in turn helped ensure that the status quo was maintained after the Tunis phase.[214]

At the beginning of the Tunis phase, Utsumi seemed to have taken a more moderate stance. In his opening statement, Utsumi contrasted the regulatory framework of the Internet with that of telephone networks,[215] which is within the ITU's sphere of influence. He noted that the traditional telephony approach in which each state regulated according to its own desires would not work for the new technology of the Internet.[216] WSIS correspondent Dick Kaser quoted Utsumi as follows:

> The value of the Internet derives from the value of the information created and consumed rather than from the structure itself. The existing [telecommunications] models do not work well. We need to embrace communications sovereignty. What matters is that everyone be guaranteed access to communications, rather than [governments attempting to] control the means of communication.[217]

By the end of the summit, however, Utsumi reversed his position and refused to accept the consensus reached at the Tunis phase.[218] In the span of a few days, Utsumi came to the conclusion that the telephone regulatory model was in fact best for regulating the Internet. At the WSIS's closing press conference, the ITU head stated, "Telephone networks are made up of regional, domestic networks united together in agreement of the ITU framework. A similar situation may start with the Internet."[219] Therefore, Utsumi continued, "the role that the ITU plays for the international telephone net-

213. Kieren McCarthy, *ITU Refuses to Accept Net Governance Agreement*, THE REGISTER, Nov. 21, 2005, http://www.theregister.co.uk/2005/11/21/utsumi_rejection/ [hereinafter McCarthy, *ITU Refuses*].

214. *See id.*

215. Kaser, *supra* note 6.

216. *Id.*

217. *Id.* (alteration in original).

218. *See* McCarthy, *ITU Refuses*, *supra* note 212.

219. *Id.*

work will be called upon."[220] Quite remarkably, Utsumi predicted that, within five years, the ITU would be called upon to take over the Internet.[221]

Statements like these indicate that the WSIS did little to change the minds of those opposed to the United States. It is understandable that Utsumi would want to expand the reach of his regulatory bureaucracy into even greater areas. Bringing the Internet under its control would be a huge coup for the ITU. What is not understandable is how Utsumi hopes to maintain credibility when he completely contradicts himself within a matter of days regarding his stance on traditional telephony regulation serving as a model for Internet regulation. Critics question ICANN's credibility, but a much greater credibility issue arises when the Secretary-General of the ITU, the very organization in charge of the WSIS, openly refutes the WSIS consensus.

The credibility of the WSIS can also be challenged based on the location it chose for the second phase of the summit—Tunisia. What kind of signal does it send when the global discussion on the Internet is hosted by a country that itself engages in Internet censorship?[222] The Tunisian government forces all Internet Service Providers within its borders to run their traffic through the Tunisian Internet Agency (ATI).[223] If ATI disapproves of a website, it just blocks access to it.[224] In an underhanded manner, ATI tries to hide the fact that it is blocking sites by using false error messages.[225] When Internet users in Tunisia try to access a blocked site, instead of getting a message that the site has been blocked, they get a fake 404 error page, which implies that the queried site does not even exist.[226] This exact type of censorship created a controversy during the Tunis phase of the WSIS when ATI decided to block "Swissinfo.org," a Swiss news website.[227] ATI's decision came in response to the site's coverage of the Swiss president's speech at the summit in which he criticized the Tunisian government's censorship practices.[228]

If organizers of the WSIS were serious about promoting the benefits of the Internet and bridging the "digital divide" by making information technologies more available, they would have held their summit in a country that actually values the free flow of information. State-of-the-art information

220. *Id.*

221. *Id.*

222. *See* Kieren McCarthy, *This is How a Government-Filtered Internet Looks*, THE REGISTER, Nov. 21, 2005, http://www.theregister.co.uk/2005/11/21/tunisia_net_filtered/.

223. *Id.*

224. *Id.*

225. *See id.*

226. *Id.*

227. *See id.*

228. *See id.*

technology is useless if a country blocks the information users seek. The credibility of the WSIS is called into question by its holding the second phase in a country so hostile to the true purpose of the Internet—the free flow of information. The Internet community should be wary of calls to internationalize Internet governance when such calls seek to give a larger role to repressive governments like Tunisia.

Despite the credibility problems of the WSIS, the language in Paragraph 68 of the Tunis Agenda stating that all governments should have an equal role in Internet governance will only embolden those who desire to see the United States relinquish its narrow oversight of ICANN and the DNS. Opponents of the U.S. and the current DNS, such as the ITU, are likely to try to use the Paragraph 68 language as a springboard for more international control of the Internet. So long as the United States remains firm, though, and reiterates that ICANN's GAC already provides for input from international governments, the U.S. should be able to maintain the status quo in respect to the current DNS.

B. Analysis of WSIS Agreement on ccTLDs

Another noteworthy agreement the WSIS delegates reached in Tunis concerned national governments' authority over country-code top-level domains. After the conclusion of the Tunis phase of the WSIS, the United Nations highlighted this agreement in a press release that stated, "Delegates also agreed that, while the Internet Corporation for Assigned Names and Numbers (ICANN) would still be in charge of technical management of the Internet, individual countries would now manage their own country-code top-level domains."[229] The actual language the delegates agreed to is not that specific, however. This language is found in Paragraph 63 of the Tunis Agenda, which stated more broadly:

> Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms.[230]

While this language seems bold at first blush, it is unlikely to produce much change in the administration of ccTLDs.

Before further analyzing the ccTLD agreement, some background on ccTLD management is necessary. A ccTLD operator is responsible for as-

229. Press Release, Secretary-General, Activities of Secretary-General in Tunisia, 13 – 16 November, U.N. Doc. SG/T/2469 (Nov. 23, 2005), *available at* http://www.un.org/News/Press/docs/2005/sgt2469.doc.htm.

230. *Tunis Agenda*, *supra* note 187, ¶ 63.

signing second-level domain names under its particular ccTLD.[231] While the Internet was still in its early stages, Jon Postel delegated ccTLDs to operators in a very informal manner.[232] In creating ccTLDs, Postel did not want to get caught up in the politics of determining what was and was not a country.[233] To avoid the problem, Postel decided which entities received ccTLDs based on a list of country codes from the International Organization for Standardization (ISO 3166-1).[234] For the most part, the first person to ask for a ccTLD delegation received it as long as Postel considered that party a "responsible person."[235] Since many governments did not yet realize the importance of the Internet, ccTLD operators were often not the governments themselves.[236] County-code top-level domains "usually fell into the hands of university computer science departments or educational and research networking organizations, rather than government agencies."[237] As the Internet has grown in importance, national governments have become much more interested in controlling the operations of their own ccTLDs.[238]

The ostensibly ground-breaking agreement on ccTLDs will probably not actually lead to any major change for two reasons. First, in order to follow the language of Paragraph 63 to the letter, the DoC would have to relinquish its contractual authority to give final approval on any additions or deletions to the root zone file. This is highly unlikely. Due to the agreement with VeriSign concerning the root zone file, any changes to the file are contingent on written approval from the DoC.[239] Consider an uncontroversial example of a change to the root zone file due to a change in a country's name (for example, Zaire changed its name to Democratic Republic of the Congo).[240] A country's name change would be reflected in the ISO 3166-1 list.[241] ICANN would then recommend removing the ccTLD that referenced the old country-code and replacing it with a new ccTLD referencing the new country-code.[242] The DoC would approve the root zone file deletion and addition,

231. *See* Yu, *supra* note 55, at 390.

232. *See id.*

233. *Id.* at 390-91.

234. *Id.* at 390.

235. *Id.*

236. *See id.*

237. *Id.*

238. Vinton G. Cerf, *Foreword* to WHO RULES THE NET?, at x (Adam Thierer & Clyde Wayne Crews, Jr. eds., 2003).

239. *See* Muller, *supra* note 11, at 717.

240. *See* von Arx & Hagen, *supra* note 40, at 41.

241. *See id.* at 40-41.

242. *See id.* at 35.

which would then be implemented by VeriSign.[243] This uncontroversial hypothetical where all the parties (the country's government, the ccTLD operator, ICANN, and the DoC) agree would nonetheless conflict with the language in Paragraph 63 because the United States would be "involved in decisions regarding another country's country-code Top-Level Domain."[244] Since any change to the root zone file must be approved by the DoC, the United States would automatically be "involved" in any decision to add or delete a ccTLD from the file. It would have to relinquish its veto power in order to strictly comply with Paragraph 63. The United States put considerable effort into negotiating that veto power, so it is highly unlikely that the U.S. will change its stance in order to strictly comply with the ccTLD agreement in Paragraph 63 of the Tunis Agenda.

The second reason why the ccTLD agreement is unlikely to produce much change is because ICANN already gives great deference to national governments regarding the delegation of who will operate their ccTLDs. Around the time of ICANN's formation, the DoC issued a policy statement in which it "acknowledged the authority of national governments 'to manage or establish policy for their own ccTLDs.' "[245] ICANN later seemed to echo this policy. In May 1999, after ICANN took over the IANA functions, ICANN issued ICP-1, which stated, "The desires of the government of a country with regard to delegation of a ccTLD are taken very seriously. The IANA will make them a major consideration in any TLD delegation/transfer discussions."[246] As recently as June 2005, when it issued its principles on the DNS, the United States reaffirmed that "[g]overnments have legitimate interest in the management of their country code top level domains (ccTLD)."[247]

243. *See id*. at 18.

244. *Tunis Agenda*, *supra* note 187, ¶ 63.

245. Yu, *supra* note 55, at 395-96.

246. *Id*. at 397-98.

247. Michael D. Gallagher, Asst. Sec'y for Commc'ns & Info., Nat'l Telecomms. & Info. Admin., Presentation at the Wireless Communications Association International Annual Conference (June 30, 2005), http://www.ntia.doc.gov/ntiahome/speeches/2005/WCA_06302005_files/frame.htm. The U.S. principles state in full:

> The United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS). Given the Internet's importance to the world's economy, it is essential that the underlying DNS of the Internet remain stable and secure. As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file.
>
> Governments have legitimate interest in the management of their country code top level domains (ccTLD). The United States recognizes that governments have legitimate public policy and sovereignty concerns with re-

But ICANN has shown the most deference to national governments by following ccTLD policy recommendations made by the Governmental Advisory Committee.[248]

On February 23, 2000, the GAC revealed its *Principles for the Delegation and Administration of Country Code Top Level Domains* (*GAC Principles*).[249] These principles have proven quite controversial.[250] The main point behind the *GAC Principles* was the assertion that national governments are the ultimate authorities over ccTLDs.[251] Regarding the role of a ccTLD operator, or delegee, the *GAC Principles* stated, "The delegee should recognise that ultimate public policy authority over the relevant ccTLD rests with the relevant government or public authority," and further declared, "The delegee should work cooperatively with the relevant government or public authority of the country or territory for which the ccTLD has been established, within the framework and public policy objectives of such relevant government or

> spect to the management of their ccTLD. As such, the United States is committed to working with the international community to address these concerns, bearing in mind the fundamental need to ensure stability and security of the Internet's DNS.
>
> ICANN is the appropriate technical manager of the Internet DNS. The United States continues to support the ongoing work of ICANN as the technical manager of the DNS and related technical operations and recognizes the progress it has made to date. The United States will continue to provide oversight so that ICANN maintains its focus and meets its core technical mission.
>
> Dialogue related to Internet governance should continue in relevant multiple fora. Given the breadth of topics potentially encompassed under the rubric of Internet governance there is no one venue to appropriately address the subject in its entirety. While the United States recognizes that the current Internet system is working, we encourage an ongoing dialogue with all stakeholders around the world in the various fora as a way to facilitate discussion and to advance our shared interest in the ongoing robustness and dynamism of the Internet. In these fora, the United States will continue to support market-based approaches and private sector leadership in Internet development broadly.
>
> National Telecommunications and Information Administration, Domain Names: U.S. Principles on the Internet's Domain Name and Addressing System, http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm (last visited Jan. 15, 2007).

248. *See* Feld, *supra* note 41, at 355.

249. ICANN Governmental Advisory Committee, Principles for the Delegation and Administration of Country Code Top Level Domans (2000), http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm [hereinafter GAC Principles].

250. *See* Kleinwoechter, *supra* note 204, at 1118.

251. *See id.* at 1117.

public authority."[252] Importantly, the *GAC Principles* also proclaimed, "With respect to future delegations or reassignment of delegations, ICANN should delegate the administration of a ccTLD only to an organisation, enterprise or individual *that has been designated by the relevant government or public authority*."[253] This stance promotes effectively giving national governments all the decision-making power to choose who will operate their own ccTLDs and relegating ICANN's authority on this issue to rubber-stamping.[254] Perhaps surprisingly, ICANN has been quite receptive to these principles.[255]

One example of ICANN's adherence to the *GAC Principles* was the redelegation of ".au," Australia's ccTLD.[256] In September 2001, ICANN redelegated the operation of .au from Robert Elz to a nonprofit organization formed by the Australian government.[257] Elz had operated the .au ccTLD since its beginning when he received the delegation from his friend, Jon Postel.[258] What was significant about this redelegation was that it came at the behest of the Australian government.[259] Such redelegations show that ICANN was already deferring to national governments in relation to the administration of their ccTLDs prior to the ccTLD agreement reached at the Tunis phase. Therefore, since ICANN is already highly deferential to the "legitimate interests" of national governments "regarding decisions affecting their ccTLDs," it is unlikely that ICANN will feel the need to make significant changes in order to comport with Paragraph 63 of the Tunis Agenda.

While ICANN's adherence to the *GAC Principles* coincides with the WSIS ccTLD agreement and should please national governments, this conformity is not without its critics. Operators of ccTLDs are wary of increased oversight from national governments.[260] The flip side of increased authority for national governments is decreased authority for ccTLD operators.[261] Stronger national government control over ccTLDs is certainly not without its downside. As one commentator reveals:

> Strengthening the "information sovereignty" of the state could encourage governments to justify restrictions of free speech and privacy in Internet communication. Strong national regulation of

252. GAC PRINCIPLES, *supra* note 248, ¶¶ 4.4-4.5.

253. *Id.* ¶ 7.4 (emphasis added).

254. *See id.*

255. *See* Feld, *supra* note 41, at 355; von Arx & Hagen, *supra* note 40, at 36.

256. von Arx & Hagen, *supra* note 40, at 36; *see* Feld, *supra* note 41, at 350.

257. Feld, *supra* note 41, at 350.

258. *Id.*

259. *See id.*

260. *See* Yu, *supra* note 55, at 398.

261. *See id.*

> ccTLDs could lead to a new level of censorship. Governments could reserve the right to instruct ccTLD managers to remove unwanted second level domains from the Internet.[262]

In fact, such ccTLD censorship has already occurred.

In a special meeting of its board of directors on July 28, 2005, ICANN approved the redelegation of Kazakhstan's ccTLD, ".kz."[263] KazNIC, the previous ccTLD operator, was replaced by the Association of Kazakh IT Companies, which had the support of the government of Kazakhstan.[264] Notably, the minutes of the meeting assert, "Agreements between ccTLD operators and ICANN are desirable but not necessary to finalize a redelegation."[265] Not long after taking control, the new ccTLD operator shut down comedian Sacha Baron Cohen's website, "www.borat.kz."[266] The site featured one of Cohen's characters, a Kazakh journalist named Borat Sagdiyev.[267] Concerning its reasoning for shutting the site down, "[t]he president of the [Association of Kazakh IT Companies] said it was so the comic 'can't bad-mouth Kazakhstan under the .kz domain name.' "[268]

Such government censorship is only likely to increase since a current ccTLD operator's consent is not necessarily needed in order for ICANN to approve a redelegation.[269] National governments now have the leverage to coerce ccTLD operators into handing over any information governments might want or censoring any website under that country's ccTLD.[270] If a ccTLD operator does not behave as the government wishes, the government can replace it via the ICANN redelegation process.[271]

C. Analysis of Internet Governance Forum

The most tangible result of the WSIS is the Internet Governance Forum. Since no real substantive change was produced during the Tunis phase and since some countries continue to harbor resentment against the United States over its influence on the DNS, the delegates basically decided to continue the

262. Kleinwoechter, *supra* note 204, at 1123.

263. Kieren McCarthy, *2005: The Year the US Government Undermined the Internet*, THE REGISTER, Dec. 29, 2005, http://www.theregister.co.uk/2005/12/29/us_undermines_internet/ [hereinafter McCarthy, *2005*].

264. *Id.*

265. *Special Meeting of the Board: Approved Resolutions*, ICANN, July 28, 2005, http://www.icann.org/minutes/minutes-28jul05.htm.

266. McCarthy, *2005*, *supra* note 262.

267. *Id.*

268. *Id.*

269. *See id.*

270. *See id.*

271. *See id.*

Internet governance discussion later through the Internet Governance Forum. The IGF is supposed to meet periodically over five years.[272] At the end of that period, the U.N. Secretary-General will make an evaluation and recommend whether the forum should continue.[273] This standing forum is likely to be the main venue for opponents of both the United States and ICANN to address their frustrations.

While a number of paragraphs of the Tunis Agenda were devoted to fleshing out the IGF, perhaps the most important was Paragraph 77, which made it clear that the forum has no real power. This paragraph stated:

> The IGF would have no oversight function and would not replace existing arrangements, mechanisms, institutions or organisations, but would involve them and take advantage of their expertise. It would be constituted as a neutral, non-duplicative and non-binding process. It would have no involvement in day-to-day or technical operations of the Internet.[274]

Paragraph 77 shows that while the IGF will provide an outlet for debate on any number of Internet governance topics, in the end the forum has no teeth. The IGF has no mechanism by which to enforce any proposals it creates.

Greece recently hosted the first IGF meeting in Athens from October 30 to November 2, 2006.[275] The forum served to keep the lines of communication open among governments, business, and civil society.[276] Additionally, the forum laid the groundwork for future meetings of the IGF. Brazil will host the next IGF meeting in Rio de Janeiro from November 12 to November 15, 2007.[277] The 2008-2010 meetings are expected to be held in India, Egypt, and Lithuania or Azerbaijan, respectively.[278] Reviewing the Athens meeting, the Internet Governance Project acknowledged that "discussions needed to be more focused and outcome-oriented," but concluded, "The non-binding discussion format succeeded in facilitating discourse and allowed nearly all participants to get something that they wanted—the airing of an issue, a chance to confer or coalesce with like-minded participants, etc. Expectations in Rio are likely to be—and should be—higher."[279]

Whether future IGF meetings will lead to any substantive change concerning Internet governance remains to be seen. These meetings will likely

272. *Tunis Agenda*, *supra* note 187, ¶¶ 73, 76.

273. *Id.* ¶ 76.

274. *Id.* ¶ 77.

275. The Internet Governance Forum (IGF) Home Page, *supra* note 194.

276. *See First Internet Governance Forum Concludes*, INTERNET GOVERNANCE PROJECT, Nov. 3, 2006, http://www.internetgovernance.org/news.html.

277. The Internet Governance Forum (IGF) Home Page, *supra* note 194.

278. *Id.*

279. *First Internet Governance Forum Concludes*, *supra* note 275.

serve as an opportunity for opponents of the U.S. to call for change regarding the United States' narrow oversight over ICANN and the DNS. In trying to get concessions from the U.S., opponents will probably point to the language in Paragraph 68 of the Tunis Agenda calling for all governments to play an equal role in international Internet governance. Nevertheless, since the IGF has no means of enforcing any decisions, the United States should be able to maintain the DNS status quo as long as it remains firm.

IX. CONCLUSION

The World Summit on the Information Society failed to produce the major changes sought by opponents of the United States and ICANN. The main outcome was that the United States did not surrender its historic control over the DNS. Opponents of the U.S. did achieve some minor victories, though. These opponents who advocated more international control of the DNS now have black and white language to help support their position. This language, found in Paragraph 68 of the Tunis Agenda for the Information Society, will give U.S. opponents more ammunition in their battle for more international control of the DNS. Proponents of increased internationalization will also try to capitalize on the WSIS agreement recognizing national governments' interests in their own ccTLDs. They will likely try to build on this to achieve increased power for national governments in other areas as well. Opponents of the United States and ICANN also now have a standing forum where they can continue to voice their opposition—the Internet Governance Forum. While the IGF has no means of enforcing any proposals it may craft, U.S. opponents will likely try to leverage the publicity it will generate to put public pressure on the United States and ICANN to make changes.

The United States should continue to resist any efforts to give other national governments more control over the Domain Name System. The U.S. gained its current oversight position due to the mountain of resources it poured in to help create the Internet and get it off the ground. International control will only lead to more problems. Consider the example of ccTLD operation, an area where the United States has already recognized other national governments' interests. Even simply giving national governments authority over their own ccTLDs can lead to censorship and abuse. In light of such problems in the isolated field of ccTLDs, it is alarming to imagine the abuses that would take place if other parts of the DNS were subjected to international governmental control.

Calls for internationalization of the DNS by countries who censor the Internet within their own borders would be laughable if they were not so dangerous. The United Nations' goal of spreading the benefits of the Internet would be furthered more by efforts to eliminate such government censorship than by efforts to grant these repressive governments even more control over the Internet. While the Internet Governance Forum will allow opponents of the U.S. to make a lot of noise, the United States still holds all the cards. The U.S. should continue to stand firm against the forces seeking international-

ization of the Domain Name System. As long as the United States does not cave in to public pressure from its opponents, Internet freedom can be preserved.