Masthead Logo

Global Business & Development Law Journal

Volume 21
Issue 1 *Symposium: I Think I Can, I Think ICANN: Regulating the Internet . . . or Not*

Article 3

1-1-2008

ICANN Internet Governance: Is it Working?

Steve DelBianco
Executive Director of NetChoice

Braden Cox
Competitive Technology

ICANN Internet Governance: Is It Working?

Steve DelBianco and Braden Cox***

TABLE OF CONTENTS

---

* Steve DelBianco is Vice President of Public Policy at the Association for Competitive Technology and is Executive Director of NetChoice.

** Braden Cox is Research & Policy Counsel at the Association for Competitive Technology.

I. INTRODUCTION

This article was originally prepared as testimony for a hearing before the Committee on Energy and Commerce in the United States House of Representatives on September 21, 2006. The hearing addressed the question, "ICANN Internet Governance: Is It Working?" This poses a seemingly simple question, although the answer is anything but simple.

This article describes some of the concerns about the management and governance of the Internet and makes several recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN) and for the U.S. Government in its oversight role. First, it clarifies that ICANN's management role is only a part of the overall Internet governance process. Next, it discusses a number of threats to ICANN's management duties. Lastly, it concludes with recommendations for the U.S. Government and ICANN to improve the Internet governance process.

II. GOVERNANCE VS. MANAGEMENT OF THE INTERNET

A. ICANN Is the Internet's Manager, Not Its Governor

It is a common perception that ICANN is engaged in Internet governance, but ICANN's stated mission is to ensure the stability and interoperability of the Domain Name System (DNS). As a non-profit organization that coordinates a number of Internet-related tasks, ICANN works in coordination with a private sector that has invested a trillion dollars to bring Internet connections to over a billion people around the world. Bearing this in mind, it is better to think of ICANN as the Internet's manager—not as its governor.

While ICANN's management focus is commonly described as "security and stability," the Internet community actually relies on ICANN to manage the DNS to achieve two key qualities—availability and integrity. Availability of the DNS is critical for anyone who relies on the Internet for information, communications, and trade. Domain name resolutions need to be available 24 hours a day, 365 days a year, from anywhere on the globe—in any language. Even the slightest degradation or interruption in DNS availability can slow or interrupt access to email and websites.

Integrity of the DNS is vital to both business and end users of the Internet. Businesses rely upon the integrity of domain name registration to ensure that their brands are not misrepresented or misappropriated. E-commerce and Internet financial transactions require integrity in resolution of domain names and secure

delivery of encrypted information. Internet users depend upon the integrity of domain name services to provide accurate and authentic results when they look up a website or send an email. Deceptive practices, such as redirecting users to fraudulent websites or providing false information about the true owner of a web domain, undermine this integrity.

Always-on availability and uncompromised integrity are necessary for a fully functional DNS and a properly performing Internet. To deliver these qualities, ICANN acts as a project manager, coordinating contracts with vendors and organizations that manage key DNS functions. These contracts and agreements are narrowly tailored and limited in scope to the terms negotiated by consenting parties.

Governments, on the other hand, are public institutions with broad portfolios and the power to compel or punish specific actions. These powers are an essential part of governing the Internet, including enforcing trademark laws, protecting consumers from fraud, and prosecuting hackers and criminals.

If ICANN were run by governments using governmental powers, the results would be predictable. Quarreling nations would find it impossible to agree on anything but the most trivial technical decisions. Developing nations would press for changes in Internet management to advance their economic development goals. Special interests would seek Internet-enabled social programs to address perceived disadvantages. It would not be a stretch to imagine a tax, or "contribution," on domain names to fund programs to "bridge the digital divide" and promote local commerce and content.

B. ICANN Management of the DNS Works (For Now)

From the perspective of businesses that rely upon the Internet for communications, information, and e-commerce, it is clear that the DNS *is working*. Customers and suppliers can quickly and reliably get to websites, buy online, check the status of an order, or just find the address of the nearest store. Over three-quarters of small businesses say their website generates leads and gives them a competitive advantage.[1] According to the U.S. Department of Commerce, online sales in the U.S. increased 23% during the second quarter of 2006 compared to the same period the year before.[2] From July 1, 2005 to June 30, 2006, e-commerce accounted for $98 billion, nearly 3% of all retail sales.[3]

This increase in e-commerce has placed greater demand on the DNS. As of November 2006, there were 112 million total domain registrations, a 30% increase over the same period in 2005. Over 9.4 million new domains were

1. *See* EMarketer, U.S. Online Advertising Revenues by Major Consumer Category, Oct. 4, 2007, *available at* www.eMarketer.com (subscription required).

2. U.S. Census Bureau News, *Quarterly Retail E-commerce Sales*, 3rd Quarter 2006.

3. *Id.*

registered in the third quarter of 2006, up 30% over the same period in 2005.[4] There were over 1 billion Internet users in 2007, compared with only 580 million in 2002.[5] International Data Corporation estimated that 1.6 billion electronic mailboxes would be in use around the world in 2007.[6]

The registry operator for .com and .net domains processed an average of 21 *billion* queries per day in the third quarter of 2006. At the end of the third quarter of that year, the overall base of .net and .com domain names was 61 million. The growth rate in the third quarter of 2006 slightly outpaced the second quarter of 2006, with 7% quarter over quarter growth and 31% year over year growth.[7] Moreover, the .com and .net domains have seen 100% uptime reliability for the past 13 years.[8]

Judging by growth and vitality, the answer is that ICANN's management is working.

III. THREATS TO ICANN'S MANAGEMENT OF THE DNS

Despite ICANN's success with respect to growth and vitality, there are several ways that ICANN's management is not working effectively to maintain the most important qualities of the DNS—availability and integrity.

A. An Overview of Attacks Threatening Internet Availability and Integrity

Seven major attacks on the DNS availability have occurred in the past six years. The largest attacks on domain name servers hijacked multiple computers in order to amplify and accelerate the assault. Last year, a distributed denial-of-service attack disabled 1,500 websites using 32,000 hijacked computers.[9] Symantec estimates that on average there were 6,110 denial-of-service attacks per day in the first half of 2006.[10] Denial-of-service attacks can cripple a website

4. VeriSign, 3 DOMAIN NAME INDUSTRY BRIEF, 2 (Nov. 2006), *available at* http://www.verisign.com/static/040029.pdf.

5. *See* Internet World Stats, *World Internet Usage and Population Statistics* (Jan. 2007) *available at* http://www.internetworldstats.com/stats.htm; *see also* Global Policy Forum, *Internet Users 1996-2002*, *available at* http://www.globalpolicy.org/globaliz/charts/internettable.htm.

6. International Data Corporation, *Worldwide Email Usage, 2003-2007: Spam and Instant Messaging Take a Bite Out of Email* (Oct. 2003).

7. VeriSign, *supra* note 4.

8. *See* VeriSign, *DNS Assurance: Product Comparison*, *available at* http://www.verisign.com.sg/dns/comparison.shtml. VeriSign manages the DNS for .com and .net.

9. Distributed Denial of Service (DDoS) attacks are conducted by controlling and compromising multiple computers—through the use of "zombies" or "bots"—to send a flood of queries against a targeted website. DDoS attacks generally overload the target's network with a high volume of traffic while simultaneously opening many web pages so that the site runs out of resources to handle legitimate requests. See http://www.symantec.com/avcenter/venc/data/ddos.attacks.html.

10. Symantec, *Internet Security Threat Report: Trends for January 06—June 06*, Volume X, Sept. 2006, *available at* http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.

and disable an online business. Moreover, these attacks can be used to *blackmail* small businesses, forcing the business owner to pay-up in order to stop the attack.[11]

Attacks on the integrity of the DNS itself are also raising alarms. Attackers can redirect web browsers and DNS servers to fraudulent sites hosting convincing scams. One method of redirection involves corrupting DNS data that is "cached" in memory so that users are pointed to fraudulent websites. Increased security measures can help, but hackers and scam artists are quick to adapt their technology and tactics.

Just how concerned are American businesses by these attacks on the Internet and affronts to consumer protection? A Zogby Interactive poll of 1,200 small businesses across the nation, conducted in May 2006, sought to answer this question.[12] The poll included questions about Internet availability and the integrity of the domain name system. Topline results from that poll tell a story in two parts. The first part shows the level of concern about Internet availability:

- 78% of small business owners said a less reliable Internet would damage their business.
- 78% said reliability and performance were more important than low fees for domain names.

For businesses that rely on the Internet for exposure and for e-commerce, threats to Internet availability are serious concerns. On the other hand, these businesses have little concern about modest price increases for domain names when that money goes towards Internet security and stability.

The second part of the Zogby poll shows that small businesses with websites are questioning the *integrity* of business practices in the domain name marketplace:

- 59% were concerned about cybersquatting—where speculators buy domain names closely related to names of real businesses and hold them for ransom.
- 69% were concerned about being exploited by registrars who charge exorbitant fees to reinstate a domain name that has been allowed to expire.

The poll findings are unambiguous—the availability and integrity of the domain name system are a concern to business owners.

---

11. Daniel Thomas, *Websites Face More Attacks—BLACKMAIL*, FINANCIAL TIMES, May 31, 2006.
12. *See* Zogby Interactive Poll, www.netchoice.org\ZogbyPoll.htm.

B. ICANN's Efforts to Promote Availability

How effective is ICANN in responding to the above-mentioned availability concerns? In its new registry operating contracts, ICANN is attentive to security and stability. These exact words appear twenty-six times in twenty-eight pages of the contract, which also declares ICANN's intention to develop new policies to improve security.[13] However, ICANN must react faster to threats and vulnerabilities. After years of study and debate, everything possible should be done to implement DNS security extensions as quickly as feasible. More importantly, security policies that help ensure availability in the face of tomorrow's threats and vulnerabilities must not take years to develop and execute. Failure to take these steps will result in lost revenue and missed new business opportunities.

Similarly, ICANN has simply taken too long to implement internationalized domain names, a step that would improve Internet availability for populations that do not use the Roman alphabet character set. This failure could prove fatal to the ICANN experiment if these populations and their governments decide to implement their own non-Roman DNS.

An available Internet is one goal of the DNS—the integrity of domain names is another. Unfortunately, as the next section will show, the integrity of domain name services is being undermined by unfair and deceptive practices.

C. An Integrity Gap in the Domain Name Marketplace

The integrity of the DNS is vital to Internet trade and consumer protection. First, businesses rely upon the integrity of domain name registration processes for the resolution of domain names and secure exchanges of encrypted information. Second, Internet users depend upon the integrity of domain name services to provide reliable results when sending email and visiting websites. Abusive, fraudulent, and unfair practices undermine the integrity that is vital to the DNS.

As manager of the DNS, ICANN can and should do more to ensure the system's integrity. Based on its consensus policies, ICANN enters contracts with registries and certifies registrars to manage the availability and integrity of the DNS. Registries contract with ICANN-accredited registrars that resell domain names and provide direct services to domain name owners. These registrars are in the best position to prevent many of the unfair and deceptive practices described below.

---

13. A draft of the contract is available at http://www.icann.org/topics/vrsn-settlement/revised-com-agreement-clean-29jan06.pdf.

1. Cybersquatting

Cybersquatting is an abusive practice in which a speculator registers a domain name identical or confusingly similar to the trademarked name of a legitimate company or organization. The speculator then holds the name for ransom, forcing the trademark owner to pay far more than the actual cost of registration just to get control of a domain name that would otherwise have no value to anyone else.

In October 2006, after just seven years of operation, the caseload of the Arbitration and Mediation Center of the World Intellectual Property Organization (WIPO) topped the 25,000 mark. Since it launched its domain name dispute resolution services, the WIPO Center has resolved disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP) and various other policies. In 2005, the WIPO Center reported a 20% increase in the number of cybersquatting cases filed compared to 2004.[14] Under the Anti-Cybersquatting Consumer Protection Act of 1999, trademark owners can sue a cybersquatter under U.S. law.

Cybersquatters unfairly and illegally take advantage of the goodwill of someone else's trademark. But for a small business, the time and expense needed to understand and assert legal claims are often more than the owner can afford. Defending a valuable trademark in court can be prohibitively expensive, especially for a small business. Consequently, most small businesses either continue to lose prospects to cybersquatters, or they pay the ransom demanded.

2. Typo-Squatting

"Typo-squatting" consists of registering domain names that closely resemble those of popular Web sites, usually common misspellings of the legitimate site name. Since almost half of all Web users prefer to type the domain name of a known website directly into their browser's address bar, misspellings are inevitable.[15] If a customer accidentally misspells the domain name she is looking for, she could end up instead at a typo-squatter's website. There she will find advertisements, often for products and services that compete with those of the legitimate site.

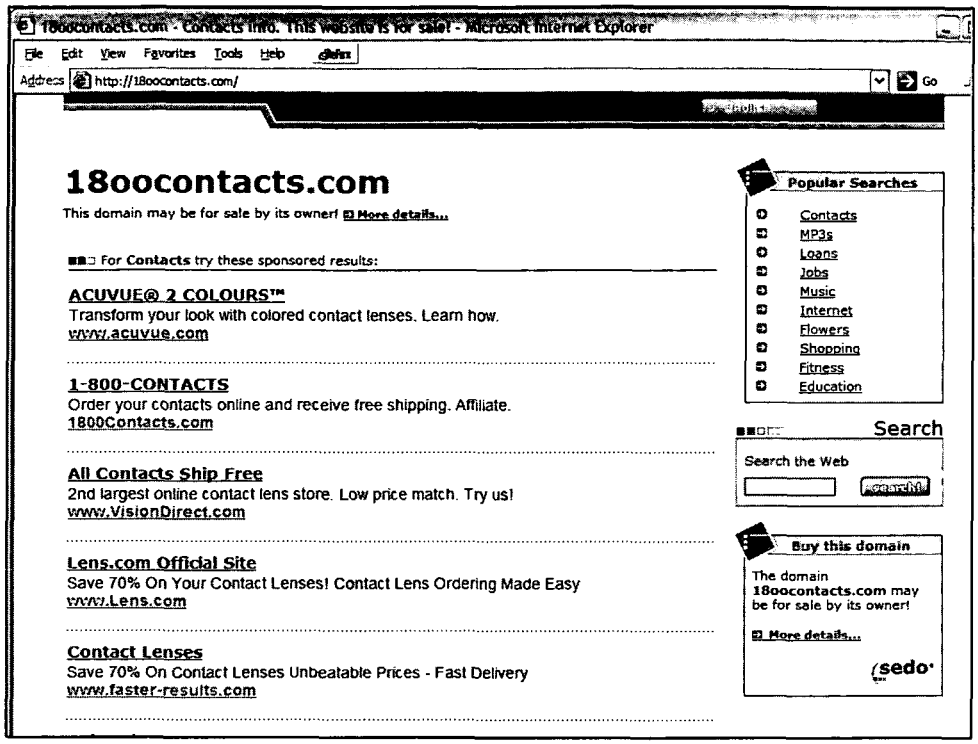
Take, for example, a few typographical variations on 1800Contacts.com, the leading telephone and online seller of replacement contact lenses. If the Web user enters 18OOContacts.com instead of 1800Contacts.com (letter O instead of numeral zero), she arrives at a page designed to steer her into buying contacts

---

14. *See* WORLD INTELLECTUAL PROPERTY ORGANIZATION, *WIPO Handles Its 25,000th Domain Name Case* (Oct. 2006) *available at* http://www.wipo.int/edocs/prdocs/en/2006/wipo_pr_2006_464.html; *see also* WORLD INTELLECTUAL PROPERTY ORGANIZATION, *WIPO Responds to Significant Cybersquatting Activity in 2005* (Jan. 2006), *available at* http://www.wipo.int/edocs/prdocs/en/2006/wipo_pr_2006_435.html.

15. Windward Directives, *North America Domain Name Study* (June 2005) (on file with author).

from competing lens sellers. 18OOcontacts.com points to a server owned by Sedo, the current leader in "parking" domain names.[16] Sedo's parking site is designed to generate advertising revenue when users who intended to go to 1800Contacts start clicking on sponsored links—*for other lens sellers.* (See screen capture shown below).[17]



> Clicking on the 1800Contacts.com link displayed on this page re-directs the user to yet another page showing ads for other lens sellers. In other words, *the hyperlink for 1800Contacts.com is falsely labeled in order to generate ad revenue from a competing site.*

Typo-squatting sites confuse and divert potential customers. When typos happen, legitimate businesses should not lose customers who fall into traps designed to generate ad revenue. Furthermore, the ad revenue generated by parking drives up the price if the intended business tries to acquire the domain from the parking operator.

---

16. For information about Sedo, *see* http://www.sedo.co.uk/about/index.php3?tracked=&partnerid=&language=e.

17. *See* http://www.18OOContacts.com/

18. EURid, *EURid Suspends 74,000 .eu Domain Names*, July 24, 2006, *available at* http://www.eurid.eu/en/general/news/eurid-suspends-74-000-eu-domain-names-due-to-breach-of-contract.

3. The Land Grab on New Top Level Domains

A similar abuse of the domain name registration system, called a "land grab," can occur whenever a new top level domain (TLD) is launched. First, speculators register thousands of names in the new domain, hoping to tie up names similar to those of legitimate businesses and organizations. Next, the speculators either demand ransom from the legitimate owner for these names or use them for typo-squatting and ad parking.

For example, when the .eu top level domain was created for Europe, speculators quickly registered names that legitimate businesses and organizations already held on other domains. EURid, the non-profit organization operating the .eu registry, consequently suspended 74,000 .eu domain names and sued 400 registrars for breach of contract.[18] A syndicate of registrars had engaged in abusive behavior by warehousing tens of thousands of .eu domain names with the obvious intent of selling them.

Critics of ICANN suggest that the organization exceeds its management role when trying to prevent and resolve domain name abuses. However, ICANN manages policies for initial registration, which is the best point for preventing squatting abuses. Furthermore, if a trademark dispute later arises, it is far more efficient to use ICANN's arbitration process, saving legal fees and reducing the time to resolve the dispute and re-assign the name.

Registrars are not doing enough to maintain the quality of the "Whois" data needed to fight squatting, fraud, and traffic in copyrighted material and counterfeit goods. ICANN needs to enforce its contracts, and de-certify registrars who fail to meet their contractual obligations to collect, maintain, and display accurate and complete Whois data.

4. "Sharking" (a.k.a. Domain Tasting)

Domain name "sharking" is an abusive practice in which speculators look for sites where they can park ads to take advantage of the five-day grace period between the time a new domain name is reserved and the time the registration fee must be paid. In April 2006, out of 35 million registrations, only a little more than 2 million were permanent or actually purchased.[19] Most likely a large portion of the other 33 million registrations were part of the sharking scheme. Speculators routinely register large numbers of potentially attractive domain names and then carefully track how many accidental hits they generate. If a site fails to generate much traffic, the speculator lets the domain name lapse without paying anything. However, if the site generates a lot of traffic, the speculator uses

19. Bob Parsons, *35 Million Names Registered in April. 32 Million Were Part of a Kiting Scheme. A Serious Problem Gets Worse*, May 10, 2006, *available at* http://www.bobparsons.com/DomainKiting.html.

it to park ads, often from one of the large managed Web advertising networks like Google, in order to generate significant revenue with no effort.

ICANN, aware of the growing abuse of the five-day Grace Period policy, held a workshop on the subject in two recent meetings. Still, it has not aggressively explored new grace period policies and restrictions to guard the integrity of the DNS from this kind of abuse.

5. Slamming

Most consumers with a telephone can remember the scourge of slamming—where resellers of long-distance telephone service switched a customer's provider, only to have the incumbent switch back, and so on. Domain name slamming works in a similar way. A registrar tricks an unwary domain name holder into unintentionally switching from one registrar to another—a costly and fraudulent endeavor. Domain name slammers often use direct mail or email spam to target domain name holders with phony renewal notices. If the domain name holder takes the bait, thinking that he is just renewing his subscription with the existing registrar, he may soon be forced to pay whatever the slammer demands or risk losing the domain name when it comes up for renewal.

In the U.S., domain name slamming is considered an Unfair and Deceptive Trade Practice and has been prosecuted by the Federal Trade Commission (FTC). In 2003, one of the largest domain name registrars, Network Solutions, settled a complaint with the FTC, admitting that it had deceived customers into switching registrars, leading them to believe they were merely renewing previous registrations.

Slamming continues, despite FTC enforcement efforts. ICANN has a more immediate and direct way to restore integrity to the domain name billing process by rigorously enforcing its Registrar contracts and de-certifying any Registrar who is caught slamming.

6. Expiration Extortion

"Expiration extortion" describes a common practice of forcing a domain owner to pay an exorbitant fee to reinstate a name that has been allowed to expire. A leading registrar, for example, charges $80 to reinstate a domain name that costs only $8 to initially register. Expiration extortion also describes the speculative game of snatching expiring domain names for resale to their former owner—or to the highest bidder.

Domain names are generally registered only for a year, although most owners renew before the year is up. Among all registrants, the average term for domain registration is 1.3 years.[20] Last year, the renewal rate for .com and .net

20. Netnation Communications Inc., 10QSB Quarterly Report, Aug 14, 2000, *available at* http://www.

domain names was 75%. That means 25% of names are not renewed, so every day there is an average of 22,000 expiring domain names released by registries.

A company called Pool.com has perfected the science of snatching domain names as they expire, or "drop." Pool runs 80 servers in Sterling, Virginia that fire into action every day when dropped domain names are released at 2:00 PM. According to Pool.com's president, Taryn Naidu, *"It's like going to the horse races every day."*[21] The race is won by whichever company, blasting multiple commands per second, snatches the dropped domain name.

Imagine if Pool.com were in the business of buying expired auto registrations instead of expiring domain names. Pool could snag the car owner's registration if he failed to renew it by the expiration date, then sell the registration back to him or to another bidder willing to pay more.

7. Parking of Generic Terms

This fast-growing practice involves registering generic names, such as "consulting.com", which have little value in themselves but can generate revenue by carrying minimal content and advertising. Unsuspecting visitors to www.antidepressants.com might think they have found a site with reliable information regarding depression medications. But in fact, there is no content—only links to paid ads parked on the pseudo-site by a speculator looking to prey on people searching for helpful information.

Parking ads on otherwise unused sites like this one is not only deceptive and confusing to the customer, but it also clutters the Internet the same way that unsightly billboards clutter the landscape along many of our nation's highways. This clutter diminishes the value of the Internet for legitimate businesses and organizations,and misleads individuals searching for meaningful information.

D. ICANN's Agreements with Registries and Registrars Can Promote DNS Integrity

Small businesses are increasingly frustrated and concerned about abusive domain name practices like squatting and slamming. Is ICANN doing enough to maintain the integrity of the DNS marketplace? Not a single one of the more than five hundred registrars has been de-certified by ICANN, despite dodgy practices by some. Dotster, one of the largest registrars, was recently sued for allegedly participating in a massive typo-squatting campaign.[22] Dotster is accused of abusing its status as a registrar by sampling hundreds of domain names that

---

secinfo.com/d1Ze2u.534.htm.

21. Peter Hum, *The New Cybersquatting: What'$ in a Name*, THE OTTAWA CITIZEN, Mar. 16, 2006.

22. Declan McCullagh, *Registrar Named in Massive Cybersquatting Suit*, June 5, 2006, http://news.zdnet.co.uk/internet/0,39020369,39273075,00.htm.

closely resemble true names and then keeping only those that generated enough traffic to justify the registration fee.

Nevertheless, ICANN seems to grasp the seriousness of maintaining the integrity of the DNS marketplace, judging by the new registry contract proposed for .com and subsequent TLD registries. In its new registry agreement for .com, ICANN indicates the potential for "prohibitions on warehousing of or speculation in domain names by registries or registrars."[23] An additional provision requires a registry operator to meet any future "consensus policy" adopted by ICANN to improve security and stability and to resolve disputes about domain names.

ICANN is managing DNS availability and integrity concerns contractually, through agreements with registries and registrars. However, a few large businesses have complained about ICANN's management of registry contracts, carrying their complaints to Washington, D.C. and requesting that the Commerce Department and the House Energy and Commerce Committee reject ICANN's new agreement to run the .com registry. They assert that these registry contracts would create "perpetual monopolies" by granting exclusive contracts with a presumption of renewal if the operator has met all performance requirements. ICANN's new contracts may not be perfect, but this criticism is misguided and self-serving.

First, an *exclusive* contract is essential to focus responsibility and accountability on the vendor running any single registry. The same is true for many outsourcing contracts that require accountability and consistency in the delivery of critical services, especially for infrastructure services that necessitate significant investments.

Second, renewal options are common in longer-term service contracts to provide incentives for making investments that improve vendor performance. For example, the operators of the cafeteria downstairs might invest in a new grill or espresso machine if they are confident that their contract would be renewed upon expiration. Similarly, landlords often give tenants a purchase option as an incentive to maintain and improve the property. Renewal options are already included in ICANN's latest registry contracts. Moreover, ICANN's new registry contracts require operators to implement any future policies adopted by ICANN to improve security and resolve domain name disputes. While such open-ended obligations could be difficult for any operator to meet, the authors would join those objecting to renewal if the incumbent registry operator failed to satisfy the contract's requirements. An exclusive, renewable contract is therefore typical for infrastructure services that require single-vendor accountability and continuity. In addition, it provides incentives for investment, even during the final years of the contract.

---

23. ICANN, Draft Registry Agreement, Section III.1(b) at 4, *available at* http://www.icann.org/topics/vrsn-settlement/revised-com-agreement-clean-29jan06.pdf.

What, then, is the real nature of this complaint? The largest registrars must approve fees that presently provide most of ICANN's funding. At the ICANN meeting in Vancouver in December 2005, the Finance Committee chair complained that ICANN expenditures were being delayed and possibly diminished because registrars had not yet approved the fees in the budget that was adopted for 2005-06.

ICANN's new registry contracts, however, would reduce the leverage held by large registrars today. When ICANN wants to make investments to ensure the Internet's security and stability, ICANN should not have to beg for a "permission slip" from registrars—many of whom have little interest in security or stability. From all appearances, this loss of leverage is why a few large registrars pressed Congress and the Commerce Department to reject the new .com contract late last year. ICANN can always improve its contracts, but complaints about a perpetual monopoly in the registry agreement are without merit.

In the end, disagreements over new registry contracts should not distract policymakers from acknowledging that ICANN's management of the DNS is working—even in the face of threats to DNS availability and integrity.

IV. POLITICAL THREATS TO ICANN'S MANAGEMENT DUTIES

ICANN's management duties are additionally threatened by outside, political forces that could become serious in the near future if ICANN fails to do its job properly or if it becomes burdened with governance duties beyond its managerial role. Two major threats are United Nations encroachment on ICANN and a potential splintering of the Internet.

A. The Threat of United Nations Encroachment on ICANN

There is a real and growing risk that the United Nations will encroach upon ICANN's technical role for managing domain names. The UN organized a World Summit on the Information Society in 2005 to discuss Internet Governance. A UN working group then released a report that included controversial policy recommendations for the future of the Internet. Thanks largely to a unanimous resolution from the United States Congress in November 2005, representatives from the international community allowed ICANN to continue managing the Internet under U.S. oversight, for the time being.

At the same time, the UN formed a new organization, the Internet Governance Forum, which met for the first time in Athens in October 2006. The program at Athens included workshops on a diverse range of societal issues, such as the "Greening of IT" and "Legal and Institutional Mechanisms which Strengthen the Capacity of Civil Society for Participation in Decision-making."

While ICANN is far from a perfect manager, it provides the needed separation between the technical operations of the Internet and governments. ICANN's bottom-up coordination of technical functions is the best way to

preserve the democratic and decentralized character of the Internet and keep it strong and independent to fend off interference from the UN and governments.

DNS control by the UN or another governmental body would have significant economic and cultural effects. The decision making process would be even slower than it is now, further delaying implementation of new technologies and processes that would benefit the DNS and its use in e-commerce. Economic development and "social engineering" projects could interfere with essential technical management functions. Some nations, most notably China, maintain censorship controls on the Internet content available to their citizens. In a government-controlled ICANN, these nations might call for technical changes to facilitate censorship, tempting other regimes to restrict content access as well. Moreover, the UN does not formally recognize the voice and vote of private sector interests that manage ICANN today.

The International Telecommunication Union's new Secretary-General, Hamadoun Toure, recently said that the United Nations will not try to take the lead in determining the future of the Internet.[24] However, it would be a risky strategy for both the U.S. and ICANN to ignore the voices of the UN and other governments. That could lead to an unlikely, though highly undesirable outcome—splintering of the Internet.

B. The Threat of Splintering of the Internet

A splintered Internet threatens everyone, not just ICANN. In the brief history of the Internet, ICANN has not always been the only keeper of the domain name system. Alternative domain name systems still exist today and, from a technical perspective, are trivial to create. The consequences of a split Internet, however, may not be trivial. A split Internet root would lead to a divide in DNS policies, which could impair information security technologies, delivery of email, secure e-commerce transactions, trademark enforcement, and other forms of consumer protection. A split is not likely, but ICANN and the U.S. Government need to be cognizant of the risk that a large nation or multi-national group could easily establish its own DNS.

V. RECOMMENDATIONS FOR THE U.S. GOVERNMENT AND ICANN TO IMPROVE INTERNET GOVERNANCE

ICANN currently manages a DNS that generally works well for businesses and end users. However, as pointed out above, the DNS is facing new attacks on availability and an erosion of integrity, calling for better contract management by

24. Toure said "It is not my intention to take over the governance of the Internet. There is no one single issue that can be dealt with by one organization alone" Frank Jordans, *U.N. Telecom Not Eying Internet Control*, WASH. POST, Jan. 12, 2007 at A14, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/01/12/AR2007011201082.html.

ICANN and greater vigilance by consumer protection officials. In addition, ICANN must withstand UN encroachment and avoid possible splintering of the Internet. These challenges could be met by ICANN and U.S. policymakers by following these recommendations:

A. The U.S. Government Should Develop a "Lighter Touch" In Its ICANN Oversight

The U.S. Government must avoid giving the international community any excuse to claim that the U.S. is being heavy-handed in Internet governance. For example, the U.S. Government is said to have unduly influenced ICANN's re-designation of registry operators for two country-code top-level domains (ccTLDs), and these instances have become legendary among critics of U.S. oversight. While there were valid reasons for the re-delegation of the Iraq and Australia ccTLDs, critics cite these instances to claim that the U.S. cannot be trusted with its oversight role. From this point forward, the U.S. should demonstrate a "lighter touch" in its ICANN oversight.

The U.S. can take a major step to alleviate these concerns by unilaterally committing to a formal, international process for changing a designated country top level domain. Countries regard their country code TLD as being under their sovereign authority, thus entitling them to designate their own registry. ICANN should respect these decisions, subject to security or stability qualifications and allowing for expedited re-designation during emergencies. The key is to balance the sovereignty interests of local communities against the need to maintain the unity, availability, and integrity of the DNS. A detailed process for this internationalization can be developed, such as the one suggested by J. Beckwith Burr and Marilyn Cade.[25]

Another area where the U.S should show a lighter touch is in the launch of new top level domains. In 2005, the U.S. Government asked ICANN to delay the launch of the .xxx domain, designated for adult content. The proposal for .xxx had already made it through the ICANN approval processes, including opportunities for governments to comment. Although Brazil and France expressed similar reservations about .xxx, critics complain that the U.S. abused its oversight role by overriding a DNS management decision that rightly belongs under ICANN's purview.

---

25. Letter from J. Beckwith Burr & Marilyn S. Cade, to NTIA regarding the Transition of the Technical Coordination and Management of the Internet DNS and Addressing System to the private sector (July 13, 2006), *available at* http://www.ntia.doc.gov/ntiahome/domainname/dnstransition/comments/dnstrans_comment0643.pdf.

B. *The Memorandum of Understanding Should Transition into a Long-Term Agreement, While Maintaining Root Server and Contract Enforcement in the United States*

The U.S. Commerce Department and ICANN have agreed to transition DNS coordination to the private sector. The latest agreement—the Joint Project Agreement—came into effect on September 29, 2006 and extends for three years a Memorandum of Understanding (MoU) between the two parties. The MoU, signed in 1998, was the U.S. government's official recognition of ICANN as a legal entity. Six previous expirations were marked by amendments to extend the MoU and specify further milestones for ICANN to fully transition to private sector management.

Repeated extensions and milestones imply that the U.S. Government will one day cede all authority over ICANN and the "master copy" of the DNS root server. The U.S. should formalize its long-term intention to keep the authoritative root distribution server physically located in the United States. This would send a clear signal that moving the root server is not an option. As with the back-stop agreements described below, this is necessary to ensure the availability and integrity of the DNS; no other purposes should be implied or intended.

For the private sector to continue its success in managing and developing the Internet, it is critical to maintain certainty and enforceability in commercial agreements with ICANN. Replacing ICANN with an international body would jeopardize registrar and registry agreements, due to the risk of being unilaterally abrogated or modified in response to a change in sentiments among ICANN participants. Furthermore, moving ICANN's place of business from the U.S. to another country risks upending contracts predicated on the application of U.S. law. ICANN's progression and maturation as in institution is important for the Internet economy, and its further growth and worldwide acceptance requires—for the time being—the consistent and reliable application of U.S law.

C. *The U.S. Government Should Maintain "Back-Stop" Agreements for Major Registry Operators and Numbering Authorities*

Since the formation of ICANN, the U.S. Government has maintained contingency agreements with operators of the authoritative root server, acting as a back-stop in case ICANN were unable to execute its current responsibilities. Prudence dictates that the U.S. continue this practice as a way to guarantee DNS availability to business and consumer interests both here and abroad.

VeriSign and the Department of Commerce have one such agreement, referred to as the "Cooperative Agreement." This agreement was modified after the conclusion of ICANN's registry contract with VeriSign.

Amendment 30 to this Cooperative Agreement obligates VeriSign to certain terms, including the following:

- VeriSign must obtain prior written approval from the Department of Commerce before execution of a renewal or substitution of a future .com Registry Agreement.
- The Department has the right to review the renewal provisions of any substitution for the new .com Registry Agreement.
- If the Department fails to approve a renewal or substitution, VeriSign becomes bound by the terms of the Cooperative Agreement, which include the ability of the Department to open a competitive process for the management of the .com registry.
- VeriSign must obtain prior written approval from the Department of Commerce before any amendments can be made to the pricing provisions of the agreement or execution of a renewal or substitution of a future .com Registry Agreement.
- Department approval of any renewal or substitution will occur only if the Department concludes that it will serve the public interest in the continued security and stability of the Internet domain name system and the operation of the .com registry.

D. ICANN and Governments Should Make the Government Advisory Committee (GAC) More Involved and Responsive

Governments are not nearly as effective as they should be when participating in ICANN policy development. Government representatives often disregard target dates established in the policy development process by failing to provide timely and responsive comments at the time when policies are being formulated. Moreover, some government comments have reflected more rhetoric than reality when characterizing the potential impact of proposed ICANN policies. Finally, ICANN decisions should not be held hostage when governments cannot reach consensus—government input should be provided, even when it does not represent a consensus position.

E. ICANN Should Improve the Reach and Transparency of Stakeholder Involvement

Whenever ICANN supporting organizations and advisory committees present their official positions to the ICANN Board and community, they should reveal the degree of consensus achieved and the range of views. ICANN should encourage constituencies and advisory committees to report voting results, if any votes were taken. More importantly, ICANN's Board should request fuller disclosure of dissenting opinions and alternatives considered.

A recent example where this form of transparency worked well is ICANN's Generic Names Supporting Organization (GNSO) Council report on alternative formulations for the purpose of Whois. As this report showed, a bottom-up process can attempt to forge consensus, but it should not suppress dissenting views. Moreover, ICANN outsiders would more readily participate if they could see any dissenting views and alternatives presented alongside majority views when constituencies provide advice to ICANN's Board.

VI. CONCLUSION

The Internet's DNS has become an irresistible target for hackers, criminals, and unfair or deceptive practices, all of which endanger its availability and integrity. ICANN has made progress in its seven year history, but it needs more operational experience to merit greater independence from U.S. Government oversight.

ICANN is a work-in-progress on the way to a bold and optimistic vision. No comparable precedent comes to mind for this multi-national, public-private partnership to manage an enterprise as complex and dynamic as the Internet. The vision that created ICANN is still worthy of the steadfast support of a world that increasingly relies on the Internet for information, communications, and commerce.