



Promoting Convenience, Choice, and Commerce on The Net

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
www.netchoice.org

July 31, 2008

Please accept these comments from NetChoice, a coalition of trade associations and global e-commerce companies, plus over 18,000 small businesses that rely on e-commerce. NetChoice works to promote the growth and viability of global e-commerce for the next generation of users and applications.

NetChoice supports ICANN's continued evolution toward bottom-up, private sector-led management of the Domain Name System, free from governmental interference or control. NetChoice applauds ICANN for actively planning to increase effectiveness and operational transparency, including the five key initiatives set forth in ICANN's *Transition Action Plan* and *Improving Institutional Confidence (IIC)* documents:

1. address freedom from capture
2. strengthen ICANN's accountability to its community
3. meet the needs of the global Internet community of the future
4. ensure Financial and Operational Security
5. maintain Secure and Stable operations

ICANN's *IIC* and *Transition* documents include some promising steps to implement these 5 initiatives. However, it is the opinion of NetChoice that ICANN's actions don't match its stated goals in these key areas of institutional confidence. The most obvious and current example is seen in ICANN's current plans for implementing internationalized domain names (IDN) for TLDs. As explained below, ICANN's 'fast track' plan for IDN TLDs is likely to erode—not improve—confidence of the private sector in the ICANN institution.

NetChoice is also concerned that the transition documents contemplate only a narrow aspect of the "freedom from capture" issue, ignoring a potentially grave threat of external, rather than internal capture. Failing to address these broader issues in advance of transition could severely and unnecessarily jeopardize ICANN's necessary commitment to ongoing, private-sector leadership.

ICANN's plans for IDNs could undermine Institutional Confidence

The evolution and current state of IDNs demonstrates ICANN's vulnerability to capture and a lack of accountability to multiple stakeholders, especially for the billions of present and future Internet users who don't use the Roman alphabet.

IDNs were already long-overdue when NetChoice attended its first ICANN meeting in 2005. Under growing pressure from businesses, users, and governments, ICANN eventually settled on a technical plan for allowing non-Roman characters in TLDs. But a handful of governments went their own way, creating their own non-Roman TLDs and doing domain registration and resolution within their own borders. This move was a wake-up call for the

ICANN community, showing that the Internet faced permanent fragmentation if ICANN didn't quickly implement a single global solution for IDNs.

ICANN's response included a test of IDN compatibility with applications such as email software and browsers. At the same time, ICANN decided to implement IDN TLDs as part of a much broader plan for introducing new gTLDs in Roman characters, too. As that larger gTLD process began to bog-down in policy debates over moral objections, contention, and rights protection, it looked as if IDN TLDs would be pushed indefinitely into the future. The entire community, including NetChoice, realized the growing risk of governments splintering the Internet, and encouraged ICANN to move more quickly with IDNs.

The ICANN community responded to this challenge by creating a 'fast track' for IDN versions of country code TLDs. Unfortunately, this fast track threatens to let governments capture the IDN implementation process, at the expense of registrants and other stakeholders and at the expense of Internet users who need to reach gTLD websites using their native alphabets.

Governments and their ccTLD operating partners are insisting on the fast track for IDN ccTLDs, knowing that these TLDs will launch long before IDN gTLDs can work their way through ICANN's approval process. Given the complexity of the new TLD approval process, the gap between fast track and the "all other TLDs" track will be many months, and possibly even years. And as we learned from the original TLDs, the first to market gains an enormous advantage over alternative TLDs that arrive only later.

If ICANN's fast track were reserved only for country-code domains, today's global domains (in gTLDs such as .com, .org, .edu, and .net) would be relegated to the slow track when it comes to reaching users of IDN scripts. As long as sovereign nations control the IDN space, websites seeking to reach IDN users have to apply for a ccTLD IDN – or they get no IDN at all. That places governments in sole control of who's allowed to own a domain name in their country-code TLDs, and allows governments to impose restrictions and conditions on those owners.

Giving total control of IDNs to governments will undermine ICANN's mandate -- to maintain private sector leadership in developing and managing the Internet's domain name system. And it undermines one of ICANN's new transition initiatives --to strengthen accountability to its community, which includes millions of registrants seeking to reach billions of IDN users.

Moreover, the fast track plan fails to "meet the needs of the global Internet community of the future", which is number 3 in ICANN's list of key initiatives for institutional confidence. For example, an Arabic user wanting to reach google.com would have to choose among 20 different variations of Google in the countries controlling Arabic versions of their country domains (Egypt, Syria, Iraq, etc.) It would be undoubtedly more natural and convenient for Arabic users to simply enter google.com entirely in Arabic. Again, this would undermine ICANN's key transition initiative to "strengthen ICANN's accountability to its user community".

Governments are insisting that ICANN create a fast track for their ccTLDs, but they refuse to grant any authority to ICANN or to enter contracts with ICANN. In its post-Paris statement, or *GAC Communiqué – Paris*¹, the GAC showed its preference for having ccTLDs launch without waiting for IDN versions of gTLDs that would be globally available. In that same *Communiqué*, the GAC reminded ICANN that governments—not ICANN—should determine

¹ GAC Communiqué – Paris, at <http://gac.icann.org/web/communiques/gac31com.pdf>

strings and registry selection. Moreover, the GAC said “it would be inappropriate for new IDN ccTLDs to be obliged to enter into contractual agreements with ICANN.”

The GAC Communique illustrates the extent to which governmental bodies can advantage themselves in the ICANN process at the expense of private-sector. It calls to mind George Orwell’s satirical observation of a world in which “*all animals are equal but some animals are more equal than others.*”

The IDN saga demonstrates how ICANN is likely to undermine institutional confidence in three of its five major transition initiatives: capture; accountability; and global needs. We are particularly concerned that the threat of capture has not been adequately addressed in the transition documents. For ICANN to maintain its global legitimacy, it must maintain its traditional commitment to private-sector management of the DNS. If the threat of capture, both from within and without, is not fully addressed prior to transition, we fear that commitment may be in jeopardy.

The Threat of Capture Takes Many Forms

The transition discussion documents devote considerable attention to "Safeguarding ICANN Against Capture," but focus almost exclusively on capture by internal elements, rather than external threats.

Ironically, ICANN already has in place some protections to prevent internal capture. Working groups and supporting organizations are structured to allow all stakeholders an opportunity to participate in the process and most can vote on ICANN policy decisions. Although these protections can always be strengthened -- and indeed must be strengthened for the next stage in ICANN's evolution -- it is the newer threat of external capture that raises the gravest concern for the business community.

Because transition contemplates a potentially significant change in the relationship between ICANN and the U.S. Government, questions arise as to whether that change will expose ICANN to external capture, either from governments/governmental bodies seeking to exert control over ICANN, or from ICANN willingly subjecting itself to external control. These issues must be fully explored and addressed before ICANN affects transition.

It is the position of NetChoice that the full range of issues relating to both internal and external capture must be fully explored and adequately addressed before transition can be effected in a manner that upholds the stability and security of the DNS.

Private Sector Leadership Must be Maintained

In the current Joint Project Agreement with the U.S. Government, ICANN recognizes the goal of continuing to develop and uphold “*private sector leadership in the innovation and investment that has characterized the development and expansion of the Internet around the globe*”².

The private sector has invested a trillion dollars to bring the Internet to a billion people, and it is the private sector that will bring the Internet to the next billion, and to the next billion after that. The global success of the Internet is directly attributable to the private sector's role in building and managing it.

² Joint Project Agreement, at www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/ICANNJPA_09292006.htm

From its inception, ICANN has sought to provide bottom-up, consensus-driven, private-sector leadership of DNS -- a goal that is even more important and relevant today than it was a decade ago. But it has become readily apparent that this goal is not universally shared. Both within the ICANN community and in the world at large, there are powerful interests committed to tipping the balance of control away from the private sector and in favor of governments.

The Threat to the Private Sector's Role at ICANN

Private sector management of ICANN and the DNS has been a paragon of success in building an ever-expanding Internet while maintaining security and stability. That model, however, is coming under increasing pressure from a handful of national governments.

A handful of national governments that are vocally critical of the current ICANN model may be motivated by the notion that anything so important as the Internet simply *has* to be managed by governments. But that view misses the fact that investment and innovation by the private sector— not by governments – has made the Internet so successful. And, it misses the fact that sovereign governments already have legal control over conduct and content within their borders, whether on the Internet or in any other medium. That is, nations still make and enforce their own laws governing freedom of expression, fraud, spam, cyber-security, and cyber-crime.

Countries like China, Russia, Iran, and Syria have been calling for an alternative to the international private sector model embodied in ICANN. Reform proposals offered in the World Summit on the Information Society (WSIS) and Working Group on Internet Governance (WGIG) would have created multi-government organizations to govern the Internet. While those proposals were temporarily shelved to create the Internet Governance Forum (IGF), they were revived by the Russian government at the Nov-2007 IGF meeting in Rio de Janeiro. Putting Internet management in the hands of governments would hinder investment and innovation, suppress free expression, and threaten the network's inherently open architecture.

Ironically, it is the *threat* – not the actual *fact* – of US Government oversight that is keeping other governments from displacing private sector interests at ICANN. Upon dissolution of the US Government's existing role in the ICANN process, ICANN could conceivably be “captured” by the governments that are today ICANN's harshest critics. Capture could happen in a variety of ways, including:

- ICANN's Government Advisory Committee (GAC) could insist upon formal voting and veto power over ICANN decisions;
- Government-run operators of country code domains (ccTLDs) could assert their numerical majority to control the Country Code Names Supporting Organization (ccNSO) at ICANN; and
- Government-run operators of ccTLDs could dominate the IDN domain space if the fast track is reserved only for country-codes.
- As ICANN launches new top level domains, some governments will undoubtedly assert control over native language versions of gTLDs such as .com and .org. The governments that operate these registries and related businesses will thereby gain voting power on ICANN's GNSO Council, where most of ICANN's policy work originates.

These are real threats to ICANN's current model of private sector management, which all agree must be preserved and protected. When the JPA expires in September of 2009, ICANN will need a long-term arrangement that protects against these and other potential threats.

Conclusion

Today's Internet is thriving, thanks to private-sector investment and innovation, not command and control by governments. ICANN's bottom-up, private sector-led structure has ensured a secure, stable, open and free Internet; and it must be enshrined and protected for the future.

The threats of capture are real, and must be addressed fully in order for the transition process to work. Unless these issues are fully addressed, "transition" could end up leading ICANN away from true private-sector management, rather than toward it.

Sincerely,

Steve DelBianco
Executive Director
NetChoice Coalition