

PLEASE, KEEP THE CORE NEUTRAL

By Michael Palage and Avri Doria

We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers.¹

Many in the technical community attribute the rapid growth and spread of the Internet to innovation that took place at the “edge” of the network, while its “core” was left largely application neutral to provide a universal and predictable building block for innovation. It is this core neutrality that provides a basis for the security and stability of the Internet as a whole. And it is this same core neutrality that is critical to the continued spread of the Internet across the Digital Divide. Unfortunately, when the politics of censorship rather than solely technical concerns drive the coordination of these “core” Internet resources, it threatens the future security and stability of the Internet. This paper proposes a paradigm upon which *all* the governments of the world have *equal access* to these core Internet resources to empower them and their citizens with the rights acknowledged in the WSIS Declaration of Principles.

PANDORA HAS OPENED THE BOX

When certain governments interjected themselves into the ICANN Board’s consideration of the ICM Registry application for an adult TLD on public policy grounds, they set in motion an irrevocable set of events that have profound consequences on ICANN’s future. The first such manifestation can be seen in the Draft GAC principles on new TLDs that have proposed the ability of a single government to block indefinitely, i.e. effectively a

¹ WSIS Declaration of Principles, 12 December, 2003; Paragraph 4

veto, a future TLD application if they had unmet public policy concerns. Recognizing the shortcomings of this draft recommendation, certain government(s) have stated they intend to advance in Lisbon a new standard by which a significant number of governments would be able to formally object to, and therefore block, a new TLD. This new standard appears to be a compromise between the current GAC principles that require consensus, and the single government implicit veto contained in the original draft GAC principles.

Regardless of what is contained in the final GAC principles on new TLDs, governments have made their intentions clear. They believe that entries into a domain name database involve public policy considerations that fall within their purview. Exercising this newly claimed right by the GAC has unfortunately put a new dimension of international politics into one of the Internet's core infrastructure components, the Root A server. Instead of governments regulating what their citizens can and cannot access at the edge of the network in their own countries, as they have successfully done to date, they are now seeking to regulate actions at the core of the Internet. Unfortunately, when governments take such draconian actions at the core, they negatively impact the ability of Internet users in other countries where there are different, and sometimes even opposite, public policy considerations.

ONE COUNTRY'S NATIONAL HERO IS ANOTHER'S COUNTRY'S JOKE

Injecting international politics into one of the Internet's core technical resources could not have happened at a worse time, as ICANN and the Internet stakeholder community are on the cusp of achieving the predictable and regular addition of new TLDs, including IDN TLDs, into the Root. If reviewing the TLD applications received in the 2000 Proof of concept round and the 2004 sTLD round is any guide, it is highly likely that controversial TLD submissions will be received in the next rounds. However, the most complex challenges will not lie in connection with applications for TLDs associated with vice or immoral behavior, but with applications for TLDs associated with political groups, religious groups, or civil society and advocacy groups within some countries.

For example, while certain political groups are involved in the majority governing body of some countries, these same political groups have been deemed terrorist organizations by other governments. Similarly there are certain civil society groups that legally operate in some countries trying to advance individual and/or personal freedoms in another country, but whose actions are deemed illegal in the country where they are trying to advance those freedoms. Any action by one of these political groups or civil society groups to seek a TLD for the community whose interests they claim to represent, poses the risk of an offended government taking actions that disrupt the unity and neutrality of the Internet.

SOLUTION: MORE NOT LESS

Given the potential Catch 22 scenario that ICANN finds itself in, the question that needs to be asked is whether any action can be taken to preserve the integrity of the root and ICANN's technical coordinating role. The answer is yes, but the solution is almost counter-intuitive. Instead of specifying the number of governments to meet a required threshold that can block a potential TLD applicant from being added to the root, the new standard should be that any applicant operating properly under the laws of the country in which it is organized should be subject only to ICANN's technical, operational and other criteria. Assuming the basic TLD application criteria and processes are met, the TLD should be added to the root.

Instead of a race to the bottom where countries would seek to align with other countries to impose their moral or political values by blocking applications endorsed by other governments, governments should encourage organizations and businesses within their own country to fully recognize the potential of the Information Society by adding new value and depth to the Internet. In the case where the inclusion of a TLD into the root zone may give rise to public policy considerations in another country, that country can

take appropriate actions at the edge of the network to protect or advance the public policy they have.²

EDUCATION IS THE KEY

Regardless of what actions the GAC takes, it is more important than ever for ICANN to educate the global community through all available fora about the implications of its limited role as a technical coordinator. In order for the goals of the Information Society to be fully achieved, it is paramount that there be a neutral coordination of the Internet's core resources. While ICANN provides a platform for universal resolvability, it should be recognized that governments do retain under their sovereign authority the right to block access to certain packets. Those countries that do block or impede this universal resolvability can either do it openly or clandestinely. Notwithstanding these actions by governments, ICANN actions in adding entries into a database should be a politically neutral technical function and as such would not interfere with the sovereign right of a government to regulate at the edge of the Internet.

2 It should be noted that the authors do not advocate or support censorship as a solution even within a national context. We also understand that it is not within our, or ICANN's, purview to direct the sovereign activities within the various GAC homelands.