Council Working Group on international Internet-related public policy issues

Fourth meeting – Geneva, 3-4 November 2014

Document WG-Internet-xxx
10 February 2014
English only

United States of America

RESPONSE TO THE QUESTION OF THE THIRD MEETING

Introduction

The United States is pleased to respond to the recent question of the ITU's Council Working Group on International Internet-related Policy.

> *Recognizing the scope of work of ITU on international Internet-related public policy matters, represented by the list of topics in Council Resolution 1305 Annex 1 which was established in accordance with decisions of ITU membership at the Plenipotentiary Conference, the Council Working Group on International Internet Related Public Policy invites Member States to provide their position on following question:*
>
> *What actions have been undertaken or to be undertaken by governments in relations to each of the international Internet-related public policy issues identified in Annex 1 to Resolution 1305 (adopted by Council 2009 at the seventh Plenary Meeting)?"*

The Internet is an essential tool for innovation, economic growth, and social discourse. Given the diversity and complexity of Internet policy issues, it is counterproductive to narrowly prescribe roles and responsibilities to distinct stakeholders, including governments. We believe a flexible approach that leverages existing multistakeholder institutions and other cooperative venues would lead to a better outcome. This approach will ensure that all considerations are taken into account, encourage broader participation, and facilitate more creative problem solving. All stakeholders have an interest in realizing the goal of an open, interoperable, secure and reliable cyberspace by developing international Internet-related policy in a collaborative manner.

We acknowledge that paragraph 35 of the WSIS Tunis Agenda defines roles for the various stakeholders including states (governments), the private sector, civil society, intergovernmental and international organizations. The United States believes that Paragraph 35 must be read as a whole in the context of the broader Tunis Agenda and the discussions leading up to it, and that the necessity of engagement by the private sector, civil society, intergovernmental and international organizations is paramount. The United States' understanding of these particular roles is informed by our democratic process and our commitment to multistakeholder Internet policymaking and governance. Governments must continue to work in concert with industry,

civil society, technical and academic experts, and others to advise on what is technically and commercially feasible to ensure the Internet continues to scale, and evolve.

Unilateral efforts by governments to regulate technical and operational aspects of the Internet or to foster the development of an indigenous ICT sector by imposing discriminatory local rules serves only to hinder the kind of investment, innovation, and competition that created today's Internet. Such efforts will also inhibit industry growth and creativity and broader economic development.

Within the U.S. we are committed to using a multistakeholder approach to address Internet policy issues that ensures transparency, fair process, and accountability. This multistakeholder approach allows policymakers to work amongst the international community to find attainable solutions to the unique challenges, particularly those challenges associated with access, content, and capacity. In addition, policymakers make it a priority to promote and protect the free flow of information online. As a priority the U.S. holds that Internet users should be able to send and receive content of their choice with limited interference, consistent with international human rights norms and conventions.

Best outcomes are achieved through the active involvement of stakeholders from industry, civil society, the technical community, and academia. With full participation by all relevant and interested stakeholders, we are less likely to adopt policies and regulations that inhibit innovation and restrict the rights of free expression. Through multistakeholder collaboration, we are more likely to grow economies, catalyse opportunities, and invigorate social discourse.

Below, we provide additional detail on existing or potential governmental activities in relation to each of the International Internet-related public policy issues identified in Annex 1 of Resolution 1305.

1. Multilingualization of the Internet Including Internationalized (multilingual) Domain Names

A logical starting place for promoting the development of local language content is for governments to encourage the development of services, applications, and websites in local languages, especially by maximizing the potential of their country code top-level domains (ccTLDs) to serve as venues for local content. Governments can also support research on improved automated translation methods as well as initiatives to scan and digitize key historical and educational materials. Most importantly, by establishing an enabling environment that encourages innovators and entrepreneurs to develop local digital content, governments can empower their citizens to take the lead on multilingualization efforts. Each of these activities can help increase the amount of locally relevant and accessible content available online. Another key consideration is the development of locally relevant content—creating the on-line value that pulls demand onto the expanding Internet. The rapidly evolving market of cloud

services, portable, personal devices and advanced software applications will power a new generation of local content as more citizens gain access to the Internet at affordable cost.

The Internet Corporation for Assigned Names and Numbers (ICANN) is continuing to facilitate the development of non-English content and the broader availability of Internationalized Domain Names (IDNs) through the introduction of ccTLDs as well as and generic top level domains (gTLDs) in non-ASCII scripts. Beginning in 2010, countries and territories that use languages based on non-Latin scripts had the ability to request top-level domains that reflect their country's name in its local script through ICANN's Fast Track IDN ccTLD process, which was developed jointly by the Governmental Advisory Committee (GAC) and the Country Code Names Supporting Organization (ccNSO). At this time there roughly 40 IDN ccTLDs have been entered into the root. A longer term IDN ccTLD policy is nearing completion.

Further, many of the first new gTLDs that have been introduced into the root of the Internet this year are IDNs, and 116 such applications have been made for strings using languages including Cyrillic, Arabic and Chinese. Governments have contributed to the development of the policies that have facilitated the introduction of IDN top level domains through their participation in the GAC.

UNESCO has primary responsibility for supporting multilingualism on the Internet, within the UN System. Governments can work through UNESCO to develop policies to promote linguistic diversity, creation of local language content, access to multilingual digital resources, use of ICTs for the preservation of languages, and cooperation with other entities seeking to promote online multilingualization. UNESCO and ICANN have also entered into a Memorandum of Understanding (MOU) to support the introduction of IDNs and to collaborate in enhancing capabilities for countries, particularly developing countries, to actively participate in building an inclusive multilingual Internet. Also of note, the Internet Society (ISOC), the OECD, and UNESCO have partnered to promote content, and to highlight the important role Internet infrastructure plays in enabling content.

2. International Internet Connectivity

Governments have an essential role to play in enabling the development of broadband networks to facilitate international Internet connectivity. The most effective way to expand networks and improve access in developing countries is by establishing competitive markets with transparent and consistent regulatory systems to attract private capital, as well as by adopting measures designed to lower – rather than increase – the cost of broadband services for end users. Crucial infrastructure for improving international connectivity includes competitive landing stations and terrestrial access points that allow numerous entities to provide service and attract international investors seeking to extend fiber networks. Attempts to finance infrastructure deployment by mandating payments between service providers will lead to demand distortions and could effectively restrict availability of Internet services and content.

There are a variety of resources available to assist governments seeking to improve international Internet connectivity, including within ITU-D where there are numerous efforts focused on broadband deployment. The World Bank, the Inter-American Development Bank, and other regional development banks can help fund improvement in connectivity by identifying additional ways to further investment in broadband infrastructure and by providing best practices and means of technical assistance. Additionally, many nations offer bilateral assistance; for example, the U.S. government's Global Broadband and Innovations program provides technical assistance in establishing national broadband plans and reforming universal service programs.

3. International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses

Governments have a number of opportunities to participate in the work of the multistakeholder entities responsible for coordinating the technical management of Internet resources, including domain names and addresses. All governments are invited to participate in ICANN's Governmental Advisory Committee (GAC), established specifically for governments to provide advice to the ICANN Board and community on the public policy aspects of issues related to the Domain Name System (DNS). Over 130 national government members, and 32 representatives from Intergovernmental Organizations now participate in GAC deliberations , and ICANN Bylaws provide that the ICANN Board must take due account of GAC advice when making policy decisions, thus guaranteeing the involvement of national governments in the management of domain name matters. The GAC also provides funding for its developing country members to participate in GAC/ICANN meetings, interpretation in the 6 UN languages is provided for every meeting, and documents are routinely translated into other languages to facilitate broad participation in GAC deliberations.

Governments have a direct and vital role in managing Internet resources with regard to the management of their national country code domains, or ccTLDs.

Governments also can play a vital role by encouraging technological updates to infrastructure, specifically for the deployment of IPv6. As Internet use continues to grow across the globe, widespread adoption of IPv6 is critical to accommodate the millions of devices which will come online. Governments can and should take an active role in working with Regional Internet Registries (RIRs) to encourage domestic IPv6 deployment. The United States strongly encourages governments to actively participate in ICANN and the RIRs, each of which manage policy development processes for their membership; there is no substitute for participation in these bodies that develop the policies related to the DNS. Governments interested in global network operations should also participate in Internet standards bodies, such as the Internet Engineering Task Force (IETF), and operational groups, such as Network Operator Groups.

4. The security, safety, continuity, sustainability, and robustness of the Internet

Governments have a responsibility for promoting the security and reliability of domestic networks in the face of an evolving threat environment. Recognizing that cybersecurity is a shared responsibility among a range of stakeholders, including government, the private sector, the technical community, civil society, and individual users, it is necessary for governments to facilitate a cooperative environment among these relevant stakeholders to manage security risk. To this end, it is necessary to establish a national cybersecurity strategy that seeks to enable such a cooperative environment to manage risk amongst the government, network operators, online commercial enterprises and users and build a culture of cybersecurity. Such a strategy should address government-private sector collaboration, incident management capabilities (such as creating a national Computer Security Incident Response Team), legal infrastructure, and education/awareness-raising.

Governments have a part to play in ensuring that domestic networks operate in a secure and stable environment. The first step towards this end is establishing a national cybersecurity strategy that encourages a cooperative environment amongst government stakeholders, network operators, online commercial enterprises, and users of the domestic network. Such a strategy should include: establishing a national Computer Security Incident Response Team (CSIRT), encouraging other domestic entities to form CSIRTs, criminalizing activities that target ICT networks, and raising user awareness through public education.

There are a number of venues that can assist governments in cybersecurity matters, including: the Forum for Incident Response and Security Teams (FIRST), the Meridian Process and Conference, the Asia-Pacific Economic Cooperation Telecommunication and Information Working Group (APEC-TEL), Asia Pacific Computer Emergency Response Team (APCERT), Organisation for American States Committee Against Terrorism (OAS CICTE). ITU-D Question 22-1/1 also provides an opportunity for member states to share national experiences and best practices related to enhancing cybersecurity.

Government representatives can work with the Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), the RIRs, and ICANN, among other industry standards groups and fora to improve security of the infrastructure through development of technical means, e.g., to improve security of the routing infrastructure, standards to secure domain names, and new methods to validate the certificate infrastructure used throughout the World Wide Web.

5. Combating Cybercrime

Combating cybercrime is an inherently governmental responsibility. Governments must therefore pass appropriate domestic laws on cybercrime, and strengthen operational domestic capacity to effectively investigate and prosecute cybercrime violations. Because much cybercrime activity is transnational in nature, each country must have domestic legislation, and continuous training for investigators and prosecutors charged with fighting cybercrime. A

country's ability to assist international partners depends on the state of its domestic law which permits cooperation with foreign partners as well as a fully trained and experienced police and prosecutor corps. Countries that may need assistance in developing robust domestic capacity on anti-cybercrime efforts should participate in regional trainings offered under the auspices of OAS, Association of South East Asian Nations (ASEAN), APEC, the African Union, the Council of Europe, and others. The United States also offers a comprehensive training program to regional organizations and foreign law enforcement partners upon request to improve anti-cybercrime capacity. In turn, the U.S. provides cooperation for data requests and joint investigations as authorized under domestic law.

The UN Office on Drugs and Crime (UNODC) is the appropriate venue for governments seeking assistance on cybercrime matters. As established by the UN General Assembly, UNODC is the sole venue within the UN system for member states to address the policy, investigation and prosecution of cybercrime, including technical assistance and capacity building to strengthen international cooperation. UNODC has established the Global Program on Cybercrime which offers both regional and bi-lateral training and technical assistance to member states to improve anti-cybercrime investigation, prosecution, and adjudication.

6. Dealing effectively with spam

The solution to unwanted spam includes the adoption of appropriate and existing technologies, the pursuit of appropriate enforcement actions against senders of spam, and the adoption of domestic laws that allow consumers to restrict their receipt of unsolicited commercial email. Filters, authentication programs, and other technologies have vastly reduced the receipt of unwanted commercial emails in regions where email providers have adopted these fundamental tools. Further, some countries have adopted laws that impose penalties on senders of spam who disregard restrictions on such mail, be they opt-in or opt-out programs.

When spam is a vector for malicious code, such as botnets, the appropriate criminal authorities, as noted above, should take action. As such, the US supports an approach that relies on the widely available and successful technologies, supported by appropriate law or enforcement regulatory action against entities that violate local anti-spam laws, finding this a proven and successful model. A number of multistakeholder organizations assist governments and other entities to control spam, including:

- The London Action Plan (LAP), a multinational forum of anti-spam enforcers, regulators and technologists. The group develops training for investigators, supports the development of anti-spam technology advances, and promotes joint law enforcement actions. Members of the LAP have brought coordinated civil cases involving global spammers and other consumer frauds. Further, the LAP, in partnership with the Messaging Malware and Mobile Anti-Abuse Working Group (M³AAWG), has developed for the OECD best practices for dealing with botnets, which often are the source of massive spam attacks.

- Internet Society (ISOC) conducts capacity building programs in developing economies on how to manage spam. In addition, ISOC has compiled relevant guidelines for technical and policy approaches to spam, and toolkits of best practices established by experts in the technology field. ISOC has bureaus in Africa, Asia-Pacific, Europe, Latin America and Caribbean, the Middle-East, and North America.
- Anti-Phishing Working Group (APWG), a multistakeholder coalition whose mission now far exceeds phishing attacks. In addition to serving as a networking resource, the APWG provides technical whitepapers and briefings from leading technology enterprises on well-established fixes for common spam-related threats.
- Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) provides technical assistance and training for the implementation of anti-spam technologies in India. It has sponsored a new training foundation to replicate this program in other regions that need assistance addressing spam and malware abuses. In addition, M³AAWG provides free on-line training, and offers printed best practices information in seven languages, in addition to English. M³AAWG's regular meetings offer unparalleled access to leading anti-spam technologists.
- Additionally, ITU-D Question 22-1/1 provides a venue for member states to share national experiences and promote best practices related to combating spam.

M³AAWG reports that despite the high volumes of spam today, its members prevent all but a relatively small percentage of this abusive email from reaching users' inboxes. According to this group, the most powerful anti-spam approaches identified to date are: 1) the widespread adoption of proven best practices based on shared industry expertise; and 2) industry collaboration in an environment of mutual trust and open dialogue.
The organizations identified above encourage all relevant entities – both public and private sector – to participation in their multistakeholder bodies, with the goal of developing a national experience unburdened by spam.

7. Issues pertaining to the use and misuse of the Internet

Please see our response the sections above on "The security, safety, continuity, sustainability, and robustness of the Internet" and "Cybercrime."

8. Availability, affordability, reliability, and quality of service, especially in the developing world

To promote widespread affordable access to the Internet, governments must enable policy and regulatory environments that are fair, transparent, stable, and predictable. Policies should promote competition, support innovation in technologies and services, incorporate education and training programs, incentivize private sector investment, and address market failure when necessary. These are the conditions that led to the Internet we have today, and these conditions must be maintained to ensure that we see continued technological innovation, diversification of services, and connectivity and access for all. A high priority is fostering an

increasingly educated and skilled workforce around the world so that the developing and least developed countries can find ways to become creators and suppliers of Internet services, applications, content, and code.

In addition, the policy recommendations for encouraging broadband infrastructure development contained in the ITU/UNESCO Broadband Commission for Digital Development Report can also contribute to more affordable Internet connectivity in developing countries. The recommendations are for governments to:

1. Provide policy leadership for investment, including open consultations on necessary policy and legal frameworks;
2. Open telecommunications markets to competition through transparent licensing regimes, opening up international gateways, and taxation reforms;
3. Enable government services that will stimulate demand for and investment in telecommunications, especially in developing countries;
4. Establish a universal service program to support broadband infrastructure investment and to eliminate the access gap;
5. Develop National Broadband Plans; and
6. Encourage efficient and innovative mobile broadband practices for new market entrants and consumers.

These recommendations warrant additional observations. Internet Exchange Points (IXPs) enable local ISPs to connect directly together and exchange domestic traffic, typically with settlement-free peering, thereby reducing or eliminating tromboning[1] and saving cost on international transit while reducing latency by avoiding local traffic to be carried internationally. Additionally; the increase in traffic at the IXP creates incentives for content providers to place their content closer to end-users by installing content caches or creating more direct routes to server hosts. Establishing IXPs would help change the business environment for local connectivity allowing services to be located closer to the users, potentially at lower cost.
In some countries, domestic policies may contribute to the high cost of international Internet connectivity, for example, in markets in which high international leased circuit prices are caused by lack of competition and liberalization.

An additional key issue is the adoption of effective Universal Service and Access Funds (USAFs) by government, and the adoption of newer technologies by commercial carriers. Combined, these provide an incentive to expand to reach rural populations through less costly solutions. Often over 50% of the population in many countries is rural; these rural populations are both expensive to serve and often have limited financial resources to afford access.
A number of international entities are available to assist governments in addressing affordability issues. For instance, the Internet Society (ISOC) provides training and assistance on developing and maintaining IXPs, which can improve service quality and reduce interconnection costs.

[1] Tromboning is a common process whereby local ISPs exchange traffic over transit routes provisioned by international backbone operators

The Alliance for Affordable Internet is a coalition of private sector, public sector, and not-for-profit organisations who have come together to advance the shared aim of affordable access to both mobile and fixed-line Internet in developing countries. Its primary goal is to realize the UN Broadband Commission's Broadband Target of entry-level broadband services priced at less than 5% of average monthly income realised. In working towards this vision, the Alliance seeks to assist many more users to come online with a particular focus on low-income countries. In particular, the Alliance has facilitated South-South dialogue to share expertise, best practices, and success stories. Also on a practical level, the Alliance has produced an outline of policy and regulatory best practices aimed at driving down the cost of internet access that is readily accessible online (http://a4ai.org/policy-and-regulatory-best-practices/).

The African Peering and Interconnection Forum addresses the key interconnection, peering, and traffic exchange opportunities and challenges on the continent and provides participants with global and regional insights for maximizing opportunities that will help grow Internet infrastructure and services in Africa.

9. Contributing to capacity building for Internet governance in developing countries

As strong supporters of the multistakeholder system of Internet policymaking and governance, the United States believes that greater participation from governments in developing countries would further enrich and ensure the vitality of the various Internet institutions. A variety of capacity building opportunities and options are available to governments through: the GAC, where developing country members can receive funding to participate in ICANN meetings; ICANN; the Internet Governance Forum (IGF); ISOC; IETF; regional and national Network Operators' Groups; and the RIRs. Information and best practices information is also provided by regional country code top level domain organizations. The Internet Governance Forum (IGF) is another source of support. Since 2005, the IGF has catalyzed partnerships between governments and other stakeholders and opened new doors for cooperation and coordination on a broad range of Internet-related public policy issues. Through workshops, sessions, and open forums – and invaluable informal networking opportunities – the IGF, in particular, has enabled governments with emerging ICT sectors to better understand how to address technical aspects of establishing IXPs, offered technical, non-regulatory solutions to spam, and considered approaches to ensuring privacy and managing risk, among other very concrete take-away benefits. Specific examples of IGF initiatives that have yielded benefits for governments include:

- Through a series of IGF workshops beginning in 2006, the cooperative work of UNESCO and ICANN on multilingualism has evolved, eventually resulting in the conclusion in December 2009 of an MOU aimed at supporting the introduction of IDNs, particularly in the developing world;
- During the 2010 IGF, UNESCO and ICANN signed a letter of intent to promote Internet access by users in Member States whose official languages are based on the Cyrillic script; and

- A workshop at the 2013 Bali IGF featured a discussion of a project in Porto, Portugal, which uses cloud computing and the Internet of things to integrate bus, train, and Metro in a city where there is a multi-modal transportation system and fiber-optical Internet backbone. Government officials actively participated in the question-and-answer period.

Understanding the cost burden of participating in numerous Internet governance activities, the United States provides grants through its Commercial Law Development Program to assist governments in attending the IGF. Similarly, ICANN offers scholarships to developing countries to attend its meetings as does the Internet Society for those interested in attending the IETF meetings as well as annual IGF. Finally, the United States Telecommunication Training Institute (USTTI), a non-profit organization offering tuition-free training to IT professionals and regulators in the developing world offers courses focused on the Internet governance ecosystem.

One of the largest challenges in ICT is training the next generation to operate and manage the infrastructure. Through programs such as Cisco Network Academy, leaders in private sector provide many times in partnership with governments have established educational programs throughout the world, and especially in developing countries, that have trained over 4 million students so that they might establish successful ICT careers.[2]
Deepening developing world participation in the various forums dealing with different aspects of Internet governance is a high priority for the U.S. Government. We strongly supports efforts of the numerous, successful multistakeholder institutions to better meet the needs of developing countries, and we welcome efforts to make the multistakeholder approach to Internet governance, standards development, and policymaking more inclusive.

10. Developmental aspects of the Internet

The Internet has proven to be a tremendous engine of economic development. One recent study estimates that when Internet penetration rises by 10 percent in emerging economies, it correlates with an incremental GDP increase of one to two percent[3]. To best seize on the developmental opportunity afforded by the Internet, governments must establish an enabling regulatory environment where competition flourishes and innovators and entrepreneurs are encouraged to participate in the digital marketplace.[4]

[2] https://www.netacad.com/web/about-us/about-networking-academy
[3] "Socio-economic Impact of Internet in Emerging and Developing Economies." The Boston Consulting Group commissioned by Telenor (2009).

[4] Lifting barriers to Internet development in Africa: suggestions for improving connectivity, The Internet Society; May 8, 2013; http://www.internetsociety.org/doc/lifting-barriers-internet-development-africa-suggestions-improving-connectivity

Governments can also use the Internet and other ICTs to help catalyze progress in traditional development projects in education, health, agriculture, and transportation.

11. Respect for privacy and the protection of personal information and data

Privacy protections are critical to maintaining consumer trust in networked technologies. When consumers provide information about themselves—whether it is in the context of an online social network that is open to public view or a transaction involving sensitive personal data—they reasonably expect companies to use this information in ways that are consistent with the surrounding context. It is the responsibility of governments to establish a system that facilitates consumer data protection while allowing businesses that provide online services to thrive.

Uses of personal data, and consumer expectations of privacy, tend to be both context- and culture-specific. The strength of the U.S. framework for consumer privacy is that it rests on widely recognized, fundamental privacy values but is flexible and adaptable to these different contexts. There are numerous privacy laws in the U.S. that protect privacy with regard to specific types of data (e.g., health data, financial data, children's data) and many different privacy enforcement authorities. The Federal Trade Commission (FTC) is the enforcement authority for several of these privacy laws and also has a general authority to protect against consumer fraud and unfair trade practices. The U.S. Commerce Department is working closely with a wide array of stakeholders to develop industry-specific codes of conduct enforceable by the FTC.

Because today's global digital economy relies on the free flow of data across national boundaries, it is important that governments work together to enhance the consistency of consumer privacy protections while still enabling consumers to enjoy the benefits of globally available goods and services. Given the contextual nature of privacy, trans-border privacy protections are best enhanced, not by attempting to harmonize national laws or trying to force nations to adhere to a single regulation, but through mutual recognition of different approaches to privacy that rest on the same fundamental privacy values, as well as enhanced cooperation between privacy enforcement authorities. The Asia Pacific Economic Cooperation (APEC) forum, for example, has made important contributions to this space with its development of the Cross-Border Privacy Regulation system and engagement with EU-based privacy enforcement authorities in implementing the concept of interoperability. This process has entailed input from numerous government and business stakeholders – from both APEC and non-APEC member economies. It potentially may yield a practical approach to ensuring privacy of cross-border data flows that respects countries' privacy regimes while minimizing burdens on global businesses.

12. Protecting children and young people from abuse and exploitation

Governments have a clear responsibility to protect children and young people from abuse and exploitation. Online exploitative behavior should be criminalized and strictly enforced. The United States has strong record of investigating and prosecuting online criminal activity that endangers children.

With respect to protecting children from online content that might be objectionable, but is otherwise legal, the United States encourages user education and awareness raising activities that give parents and guardians (as end users) the tools they need to encourage responsible online behavior and protect children. The United States strongly supports such voluntary and collaborative efforts that empower users and protect children without filtering or blocking content.

There are a number of international resources to assist governments in establishing criminal frameworks and protecting children online. UNODC is the sole venue within the UN system for member states to address the policy, investigation and prosecution of cybercrime, including crimes against children. Global Alliance Against Child Sexual Abuse Online is a joint initiative by the EU and the United States, which was launched in December 2012. Over fifty countries are now participating, and have committed to step up their efforts to protect children from online sexual exploitation. ITU-D's Question 22-1/1 provides a venue for member states to share national experiences and discuss best practices in protecting children online.