International internet Policy Priorities

United States Department of Commerce, National Telecommunications and Information Administration (NTIA) [Docket No. 180124068–8068–01] RIN 0660–XC041

The Internet Governance Project (IGP) is a group of professors, postdoctoral researchers and students hosted at the Georgia Institute of Technology's School of Public Policy. We conduct scholarly research, produce policy analyses and commentary on events in Internet governance, and bring our ideas and proposals directly into Internet governance processes. We also educate professionals and young people about Internet governance in various world regions.

IGP welcomes NTIA's broadly focused NOI on "International Internet Policy Priorities." We believe that agency is asking many of the right questions and appreciate its desire to look for guidance from the public. Our response will follow the template of the NOI.

I. THE FREE FLOW OF INFORMATION AND JURISDICTION

A. *What are the challenges to the free flow of information online?*

There are two distinct challenges to the free flow of information. The biggest and most fundamental is *alignment,*[1] which is related to the issue of jurisdiction. Alignment refers to the attempt by national governments to assert sovereignty over cyberspace, by imposing exclusive territorial jurisdiction and national controls in a globally interoperable cyberspace. Data localization is one obvious example of a policy that seeks to achieve alignment, but the process is evident in multiple domains of Internet governance: in cybersecurity policy, trade policy, intellectual property protection and content regulation. In each case states erect barriers that

[1] The concept of alignment was described in the book *Will the Internet Fragment?* (Polity Press, 2017).

attempt to create territorialized restrictions on the availability of content, services, applications, equipment and investment. All are driven by the same fundamental factor: the desire of territorial states to reassert control over information in a globally interconnected Internet. The contradiction between the globalized connectivity of the Internet and the territorial nature of state sovereignty makes alignment impossible to achieve fully, however. And so as states pursue alignment we get an inefficient duplication of cloud facilities, the balkanization of services, and/or broad assertions of extraterritorial authority, such as in the case of the "Right to be Forgotten."

A second major challenge to free flow is the growing tendency of governments to impose content policing duties on internet intermediaries. Governments who want to achieve their policy objectives in a globalized environment will often put pressure on the major Internet platforms with global reach. The problem here is twofold: first, the platform may need to fragment its services on a national basis to avoid globalizing restrictions that should only be local; second, as a private actor, the platform is often exempt from constitutional constraints regarding civil liberties and due process. When these private platforms are diverse and competitive, private content moderation is less of a problem, because users have alternatives and can vote with their feet. But in many cases the platforms are responding uniformly to pressure from governments rather than from the market or their users. Intermediary responsibility interacts with alignment frequently, as multiple states may seek to impose different, inconsistent forms of pressure on the major transnational platforms, forcing the platforms to align their service profiles with national borders.

B. *Which foreign laws and policies restrict the free flow of information online? What is the impact on U.S. companies and users in general?*

D. *What are the challenges to freedom of expression online?*

Our answer groups together free flow and free expression concerns, as they are closely related and interdependent. Sadly, a growing number of laws and policies impinge on free flow of information and free expression. They fall into the following categories:

- Data localization laws
- Censorship laws and policies
- Intellectual property laws
- Cybersecurity laws and policies
- Intermediary liability requirements

We cite here only a few examples:

- Germany's Network Enforcement Act, known as NetzDG, compels social media companies to remove hate speech and other illegal content. According to Human Rights Watch, the law "is vague, overbroad, and turns private companies into overzealous censors to avoid steep fines, leaving users with no judicial oversight or right to appeal." The burdens of compliance with this law, and the risks of noncompliance, fall

disproportionately on US-based social media companies trying to maintain a global presence. Smaller providers are unable to assume these burdens.

- A Vietnamese cybersecurity law just passed by its National Assembly contains data localization as well as censorship provisions. It requires foreign internet companies to store data within the country and open local offices. It would require social media companies in Vietnam to remove offending content from their platforms within one day of receiving a request from the Ministry of Information and Communications. They will also be required to disclose to the government the data of users suspected of anti-state activity. These provisions discourage foreign internet companies from serving Vietnamese customers, while blocking access to foreign and domestic information sources and suppressing the participation of Vietnamese businesses and users from engaging in dialogue with users around the world.

- China has passed a similar cybersecurity law, with heavy restrictions on foreign investment in and operation of cloud services. In includes data localization provisions and monitoring and restriction on outgoing data flows.

- Articles 11 and 13 of Europe's proposed Copyright Directive will be voted on July 5. These regulations would radically alter the balance of rights to favor copyright holders at the expense of the public's right to access information and the services of online intermediaries. Article 11 targets links and snippets gathered from online news sources. Article 13 imposes a new obligation on platforms to obtain licences for content uploaded by users, or to prevent the availability of such content by algorithmic filtering. According to a statement by independent academics, "Article 11 will create potentially very broad rights of ownership in news and other information that will change the way news is disseminated. This will impede the free flow of information that is of vital importance to democracy." The group also noted that "Article 13 motivates firms to use cheap upload filters which will block legitimate content. Complaint and redress mechanisms are insufficient to cope with this problem. Expressions such as permissible parodies will be affected."

- Excessive intellectual property protection can indirectly undermine the free flow of information. By insisting on stronger IPR protections in free trade agreements without appropriate limitations and exceptions, the U.S. has generated opposition to FTAs among its trading partners and transnational civil society groups. It is no accident that the IPR chapters in the Trans-Pacific Partnership (TPP) were discarded after the U.S. withdrew. All the other partners quickly ratified TPP. Linking expansive IPR protection to FTAs that affect the free flow of information (such as e-commerce chapters) can act as a barrier to agreements that would enhance the free flow of information.

Any national law that blocks or filters content has global effects, because it denies external information sources and businesses from accessing users/customers in that territory. For

companies, the effect is similar to a trade barrier in information services. For users, the effects are fewer choices of information resources, weaker competition and less diverse content.

C. *Have courts in other countries issued internet-related judgments that apply national laws to the global internet? What have been the practical effects on U.S. companies of such judgments? What have the effects been on users?*

Perhaps the most egregious example of extraterritorial effect of a court decision is the so-called right to be forgotten (RTBF). The Court of Justice of the European Union in 2014 ruled that individuals under certain conditions can request the removal of links from search results. Clarifications were sought from Article 29 Working Party which issued guidelines concerning this ruling and stated that the ruling was applicable to all relevant domain names including .COM.[2] The ruling is not confined to searches made from the Google.ES domain or to other Google sites in European ccTLDs or gTLDs. RTBF has forced search engines which are primarily American to provide a process for removal of links from their search results. Other countries such as Indonesia and South Korea have also followed suit and implemented the RTBF. This so-called "right" can lead to severe limits on access to factual information and can be abused by individuals to escape accountability[3] or to harass publishers of controversial content. Smaller search engines that do not have the capacity to provide such removal services and comply with the law might also be affected.

F. *What role can NTIA play in helping to reduce restrictions on the free flow of information over the internet and ensuring free expression online?*

G. *In which international organizations or venues might NTIA most effectively advocate for the free flow of information and freedom of expression? What specific actions should NTIA and the U.S. Government take?*

H. *How might NTIA better assist with jurisdictional challenges on the internet?*

We try to address all three of these questions together in the following paragraphs. We focus on trade, ICANN and sovereignty.

Trade.

Many limits on the free flow of information and free expression can be addressed internationally as trade barriers. Much of the content and platforms that are blocked by censors is provided by commercial information service providers who are denied market access. We understand that NTIA does not have primary responsibility for trade policy, but the expertise of its Office of

[2] Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, 16 Dec 2015. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf

[3] Sophie Curtis, "Politician, paedophile and GP claim 'right to be forgotten'," The Telegraph, 15 May 2014 https://www.telegraph.co.uk/technology/google/10833894/Politician-paedophile-and-GP-claim-right-to-be-forgotten.html

International Affairs (OIA) in international ICT policy should be put at the disposal of trade negotiators and policy makers in the U.S. administration.

We encourage the NTIA to utilize more open, multistakeholder processes to provide input to trade negotiators. Trade agreements tend to be dominated by a few special interest groups, leading to results that are not acceptable to a broader set of stakeholders.

Within WTO, the U.S. should initiate dispute resolution procedures against China's Great Firewall. China's overwhelming system of content blocking can be accurately characterized as a disproportionate response to China's concerns with specific web pages or messages. WTO rules require issues regarding national security and public morals to be handled in the least protectionist way. It is evident that China's indiscriminate blocking of entire domains does not meet that standard. While China's record of compliance with adverse WTO DRP decisions is not good,[4] the challenges often do lead to some concessions and some limited movement in the right direction.

The U.S. should join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Once in, Vietnam's data localization law could be challenged as a clear violation of the E-Commerce chapter. In addition to ICT services, the agreement would benefit the U.S. in a number of different industry sectors. Now that the intellectual property chapters have been discarded, a great deal of civil society and internet industry opposition to the agreement would be gone.

ICANN and DNS.

Within ICANN, NTIA needs to appreciate the potential for ICANN's power over domain names to be used to limit free expression. Since other governments often support using ICANN to limit free expression, NTIA should use its presence in the GAC to keep ICANN away from content regulation. ICANN's new bylaws explicitly prohibit it from extending its control of domain name assignment into regulation of web site content.[5] The NTIA needs to uphold this bylaw in the GAC and educate other GAC members of its importance. Many actors in the ICANN environment are still attempting to use Section 3.18 of the Registrar Accreditation Agreement to push ICANN into content regulation.[6] Copyright and trademark interests want registrars to respond to reports of illegal activity by suspending the registered name holder's domain name without any formal determination of illegality via governmental due process. IGP and other advocates of Internet freedom do not want registrars to take down domains based only on abuse complaints, as the registrar is not the appropriate party to determine whether a registered name holder is engaged in illegal activity. Only legal authorities following due process should be authorized to do this.

---

[4] https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf

[5] Bylaws for ICANN, Article 1, Section 1.1 (a),(b) and (c) https://www.icann.org/resources/pages/governance/bylaws-en/#article1

[6] Intellectual Property Constituency letter to ICANN https://www.icann.org/en/system/files/correspondence/metalitz-to-marby-17jun16-en.pdf

Additionally, NTIA should support ICANN's implementation of the Cross-Community Working Group recommendations on Jurisdiction. These recommendations call upon ICANN to pursue general licenses from the Office of Foreign Asset Control (OFAC) to cover transactions integral to ICANN's role in managing the DNS and contracts for Internet resources. A general OFAC license (not applicable to specially designated persons or SDNs) would facilitate global acceptance of ICANN's role as provider of legitimate and neutral domain name governance. Although we understand that the U.S. Treasury Department issues general licenses, NTIA's active support would be helpful.

Sovereignty.
The NTIA should address the challenge of Internet/nation-state alignment by promoting a view of cyberspace as not subject to national sovereignty. Consistent with its support for ICANN, which is a non-sovereign, nonstate actor-based governance regime, NTIA should help aim towards a global cyberspace governance regime analogous to ocean and outer space, which is designed to maintain the freedom of action of all nonviolent parties in a shared space. Just as the U.S. has fought for freedom of navigation on the high seas and opposed territorial and military claims on outer space, the U.S. should fight for freedom of navigation in cyberspace. NTIA should work within the administration, the ITU, the OECD and the G20 to challenge sovereignty-based conceptions of cyberspace and lead other states into a recognition of cyberspace as a "global commons"[7] which cannot be owned or controlled by any one state. We recognize that physical layer Internet infrastructure and many services are not common property; the Internet standards and protocols, however, are both non-rival in consumption and nonexclusive, and thus create a global cyberspace commons which is open to use by all.

II. MULTISTAKEHOLDER APPROACH TO INTERNET GOVERNANCE

We have re-ordered the questions in this section. We begin with the question about the IANA transition, and then move to the more general questions about the performance and future of the "multistakeholder approach." We do this because the IANA transition epitomizes the multistakeholder (MS) path on which ICANN and its community embarked in 1998. Once one understands the rationale for the IANA transition and the reasons why it should not be reversed, it is easier to understand the present and future of the "multistakeholder approach" to Internet governance.

D. *Should the IANA Stewardship Transition be unwound?*

No. The transition exemplifies what made the Internet great, and why the United States was, and to some extent still is, a principled and positive force in global Internet governance.

[7] A global commons is defined as "domains or areas that no one state controls but on which all rely." The concept applies to the standards and protocols commonly used by all participants in cyberspace - it does *not* imply that the facilities or services of networks or users are common property.

That there should be an IANA transition was U.S. policy from the beginning. The intention to relinquish US government control of IANA and move it to an accountable, private sector-based nonprofit was articulated clearly in the 1998 NTIA Statement of Policy that led to the creation of ICANN.[8] The NTIA White Paper followed on the heels of the successful privatization of the Internet backbone in 1995, which transitioned control of routing and bandwidth from the U.S. National Science Foundation to the private sector. That move led to the flourishing of a vibrant, competitive and world-leading Internet service provider industry in the U.S. Around the same time, the U.S. Supreme Court struck down an attempt to censor the Internet, and Congress passed the Section 230 immunities for Internet platforms. All these actions gave private actors on the Internet a great deal of freedom to catalyze a global user base, self-govern and innovate. If the US has a world-dominant Internet industry now - and it does - these early moves are a big part of the reason. All of them share a consistent pro-freedom, pro-market, pro-innovation thrust.

The privatization of IANA was a critical part of that bundle. During the creation of ICANN, the U.S. government, like most civil society actors and businesses, favored governing the domain name system (DNS) by a transnational community of Internet users and providers as opposed to regulation by nation-states.[9] There were and are highly practical reasons to favor an IANA run by nonstate actors. The Internet's unique identifiers (domain names, protocols and IP numbers) foster global connectivity, which is the most valuable feature of the Internet. Policy and coordination for these identifiers, and particularly the management of the DNS root zone, must be globally consistent. By creating a transnational regime rooted in private actors, the U.S. fostered uniform, technically-informed governance of DNS, while avoiding the fragmentation of regimes based on multiple national laws. It managed to achieve this global scope without resorting to international treaties and intergovernmental organizations. Globalization through privatization was the appropriate mechanism. The IANA transition was the culmination of that process. It was an attempt to follow the trail blazed by the Internet's developers and their organic governance institutions (such as the Internet Engineering Task Force and RIPE-NCC).

This new governance model was not welcomed by most foreign governments, especially the authoritarian ones. The UN World Summit on the Information Society (2002 - 2005) set into motion a long-term conflict between advocates of Internet governance through transnational nonstate actors, and traditionalists who supported national sovereignty and intergovernmental institutions. During this struggle it became evident that U.S. control of the ICANN regime was inconsistent with the principles underlying the MS governance model. In a regime based on non-state actors, one state (the U.S.) was vested with uniquely decisive powers over ICANN

[8] The NTIA White Paper stated: "The U.S. Government is committed to a transition that will allow the private sector to take leadership for DNS management. Most commenters shared this goal. ...The U.S. Government would prefer that this transition be complete before the year 2000. To the extent that the new corporation is established and operationally stable, September 30, 2000 is intended to be, and remains, an 'outside' date."

[9] The NTIA White paper stated: "...the U.S. continues to believe, as do most commenters, that neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses."

and the DNS root. That contradiction emboldened advocates of government control. If the U.S. had a legitimate role as supervisor of ICANN, why shouldn't all other sovereign states have the same oversight authority? This question ate away at the legitimacy of the ICANN regime for more than a decade. It allowed authoritarian states such as Russia, China, Cuba, Iran and Saudi Arabia to complain that multistakeholder governance was just a fig leaf for U.S. control. It risked alienating democratic "swing states" such as India, Brazil, and even the Europeans. After the Snowden revelations, the U.S. government's pre-eminent position threatened to splinter the entire Internet. The issue is not whether the IANA transition should have happened, but why it took so long.

Today, the Internet and the online economy are still riven by a conflict between advocates of the free flow of information and advocates of territorial state control. By attacking or questioning the transition, certain elements in the Trump administration seem to be saying that the U.S. does not know which side it is on. This confusion needs to be resolved, immediately. The NTIA must continue to uphold an Internet governance model based on nonstate actors, and that includes 100% support for the permanence of the IANA transition.

Far from "giving up" something post-transition, the U.S. has found that its original policy has been vindicated and gained strength. Claims that Russia and China would dominate ICANN and the DNS once the transition happened are now exposed as laughable scare talk. No such threats have emerged, and no hint of them is on the horizon.

"Unwinding" the transition is just a euphemism for what would be a divisive, wrenching and destructive reversal of 3 years of the community's work and a negation of the fundamental principles underlying ICANN's governance model. Aside from being a bad idea, it faces severe practical difficulties. Legally, there is no simple and direct way for the US government to undo the transition. US control of ICANN was based on a set of contracts between ICANN (which performed the IANA functions) and Verisign (the Root Zone Maintainer). The contract with ICANN is now terminated. Verisign has contracted with ICANN to accept its modifications to the root zone without U.S. involvement. There is no way to compel ICANN to re-sign or revive the terminated IANA contracting process. There is no way the community involved in ICANN would approve it.

Therefore, the only way to reassert control over the root of the domain name system is to:

1. Pass legislation regulating ICANN and Verisign in ways that compel them to use a US government-controlled DNS root; and
2. Pass legislation regulating all U.S.-based Internet service providers, DNS providers, hosting providers and content distribution networks to point to a DNS root zone the content of which was controlled by the US government

Given the size and importance of the U.S. in the overall internet economy, such a move would be a gigantic step toward a government-controlled, nationally aligned "internet." Let us not use any euphemisms in describing such legislation. It would be an attempt to "take over the Internet"

by one government and would be perceived as such by the rest of the world. Laws that blatantly nationalize a global facility would generate strong countermeasures in the internet community. We could expect the following things to happen:

- ICANN's legitimacy as the nexus of DNS governance would be completely destroyed. Its multistakeholder community would fall apart, as participants realized that their decisions and policy making processes no longer matter, as they could be superseded by U.S. laws and politics. Its status as an independent, transnational body for making policy would be lost.
- Russia, China and other authoritarian states would claim, correctly, that the U.S. was trying to grab control of the Internet. Other governments would be encouraged to intensify alignment processes, including setting up an alternative DNS root and inviting the rest of the world to join them. While an alternate root would never work under current circumstances, it just might work if the U.S. tried to snatch back IANA. Furthermore, foreign governments would claim, again with justification, that the U.S. was following an sovereignty-based model that vindicates the Chinese and Russian approaches. Their claims that the multistakeholder approach doesn't work would be confirmed; the U.S. action would show that we need to govern the Internet based on national sovereignty.
- As part of its accountability reforms, IANA is now detachable from ICANN. An attempt by the U.S. to nationalize IANA could prompt a move within the ICANN community to separate IANA from ICANN and find a new home for it in another organization and another jurisdiction. Root server operators in Sweden, Japan and/or London could offer to host a new DNS root, free of U.S. government control. Many of the world's ISPs would be amenable to this idea if a U.S. government took such a precipitous action.

Against these negatives, it is difficult to see what tangible benefits would come from a takeover of the DNS root by the United States government. U.S. government control of DNS root entries does not make the Internet work better technically. The U.S. could dictate policies to ICANN, but ICANN would no longer have global influence. The economic and social value of the Internet root depends on its ability to foster compatibility and cooperation among Internet users and service providers everywhere in the world. What we need here is not America First but worldwide communication first; global compatibility first. Claiming that the U.S. "owns" the root is as unproductive as claiming that the U.S. owns the high seas or outer space. Such claims provoke inter-state conflict without actually facilitating beneficial national control of anything. Just as one cannot "own" or "control" the high seas or outer space without committing oneself to endless, extensive and inconclusive military conflict, so one state cannot attempt to "own" or "control" the coordinating mechanisms of the Internet's infrastructure without committing itself to endless cyber, diplomatic and economic conflict with other states.

A. *Does the multistakeholder approach continue to support an environment for the internet to grow and thrive? If so, why? If not, why not?*

B. *Are there public policy areas in which the multistakeholder approach works best? If yes, what are those areas and why? Are there areas in which the multistakeholder approach does not work effectively? If there are, what are those areas and why?*

The defining characteristic of the "multistakeholder approach" is that nonstate actors hold governance authority. Multistakeholder (MS) governance is unique and important not because multiple stakeholder groups are involved - business and civil society are often engaged in and consulted by intergovernmental and national institutions. MS governance is important in Internet governance because policy making decisions are made by a transnational community of individuals and organizations connected via the Internet, and not by governments. Aside from this defining feature, there are huge differences in the methods and forms of what we call multistakeholder institutions. The IETF's processes are based on the actions of nominally unaffiliated individuals. There is no attempt to establish representational structures for countries, geographic regions, industries, or stakeholder groups, and there is no membership and no voting in IETF. ICANN's policy development process for domain names, on the other hand, gives distinct interest groups (trademark holders, noncommercial organizations, registries and registrars) distinct constituencies and a defined number of votes on a Council. The Regional Internet Registries are organized like membership-based trade associations but with open, IETF-like policy working groups. But whereas compliance with the standards developed by the IETF is entirely voluntary, the contractual mechanisms of the RIRs and ICANN are legally binding. The only common element across these institutions is the absence of state actors in an authoritative decision making role.

Given this understanding of multistakeholder governance, the answer to question A is yes, absolutely, the MS approach continues to be an essential part of an environment that enables the internet to grow and thrive. It needs to be strengthened and protected against the encroachment of states.

With respect to question B, the answer is much more complicated. In essence, the answer is that the MS approach works best when the scope of governance needs to be global or transnational, that is, when it needs to overcome the territorial fragmentation of state authority. Private sector-led MS institutions can achieve global governance without the paralyzing geopolitical rivalries and jurisdictional conflicts of governments. Thus, MS institutions should continue to be the preferred method in DNS governance, IP address governance, and Internet standards development, routing and most aspects of cybersecurity.

Despite current tendencies toward nationalization, the MS approach should take the lead in most areas of cybersecurity. Cybersecurity threats are global in scope. While national governments can and should take steps to secure their own national networks and information resources, the security of the overall cyber ecosystem needs to be governed in a multistakeholder manner. IGP considers various forms of networked governance used within the Internet industry to promote cyber security, such as threat information sharing and ad hoc forms of cooperation to respond to incidents and threats, to be in the broad category of governance by

nonstate actors, and hence "multistakeholder." When cooperation to solve problems needs to be rapid, flexible, transnational, and closely tied to operations, then networked governance is usually the best way. It is worth noting, however, that in these situations formalized multistakeholder institutions that put too much emphasis on process and representational categories can be inefficient and ineffective.

IGP believes that the MS approach, as defined above, can be extended into new areas. In particular, IGP is exploring the feasibility of an international attribution organization rooted in non-state actors. This idea, first proposed by the Microsoft Corporation as one of three elements in its "Digital Geneva Convention" proposal, could be realized through a consortium of academic cybersecurity and Internet policy experts, private internet operating firms from various parts of the world, CERTS, CSIRTS and private security firms.

C. *Are the existing accountability structures within multistakeholder internet governance sufficient? If not, why not? What improvements can be made?*

There are still flaws in the accountability mechanisms of the Internet institutions. Most of the RIRs, particularly RIPE-NCC and ARIN, are sufficiently accountable to their stakeholders. AFRINIC is suffering from serious organizational flaws that need to be addressed, but that is outside the scope of this proceeding.

ICANN's accountability mechanisms were improved by the new bylaws created by the IANA transition. But it still suffers from a very strong tendency of ICANN Org (i..e, its CEO and staff) to usurp the policy making role of the community. ICANN's board does not seem to be exercising oversight and control of ICANN legal or its CEO; in fact, the influence seems to go the other way. ICANN Org often takes actions and policy initiatives without full Board deliberation, deabte and approval. An example of how the ICANN Org can pre-empt community policy making is the current Framework Elements for Unified Access Model for Continued Access to Full WHOIS Data" that was issued by ICANN June 18, only a few days before its Panama City meeting. With redactions of some sensitive Whois data forced on it by the implementation of the European General Data Protection Regulation, ICANN Org has developed its own access model and has unilaterally posited who will be involved in developing the model (GAC, ICANN Org, and the EDPB, with the GNSO excluded). It has also stipulated an arbitrary timetable for that access model to be developed. This is a clear violation of the bottom up multistakeholder model.

E. *What should be NTIA's priorities within ICANN and the GAC?*

NTIA's top priority in ICANN should be to reform and restrain the GAC. The GAC must become an Advisory Committee as originally intended and steered away from the ambitions of some governments to make it an alternative, dominant policy making organ. In recent years, GAC has frequently attempted to expand its role and powers within ICANN. Its members openly seek to make governments more important than consensus policies developed within the ICANN community. At the same time the competence of the GAC - its ability to arrive at policy

conclusions that take account of all stakeholder views within a reasonable period of time - falls short. GAC has strategically exploited the bylaw which requires the board to take its advice into account to proffer policy prescriptions at the end of a policy process that ignores the work of the multistakeholder community or attempts to reverse hard-fought compromises made within the GNSO. Often GAC is lobbied by special interest groups to gain policy victories that could not be achieved in the legitimate, balanced multistakeholder process of the GNSO.

The GAC should offer non-binding advice for the board to evaluate, and not attempt to override the processes and decisions of the multistakeholder GNSO. During the IANA transition a change was made that clarifies the meaning of GAC advice and requires full consensus (defined as non-objection by any member) to issue "advice." Now that GAC advice requires true consensus, we urge the U.S. government to openly object to inappropriate or wrongheaded GAC advice. This includes GAC interventions that conflict with ICANN's status as a nonstate governance regime, or core U.S. values regarding free expression, privacy and due process.

F. *Are there any other DNS related activities NTIA should pursue? If yes, please describe.*

As already noted above, NTIA should support constitutional rights to free expression and ICANN's new bylaws by de-linking ICANN's domain name policies from content regulation. It should also facilitate ICANN's acquisition of a general license that exempts ICANN's contracted parties from OFAC sanctions in most cases.

G*. Are there barriers to engagement at the IGF? If so, how can we lower these barriers?*

H. *Are there improvements that can be made to the IGF's structure, organization, planning processes, or intercessional work programs? If so, what are they?*

The IGF is teetering on the brink of failure. IGP, like many other groups, is reassessing its willingness to continue attending and participating in IGF.

IGP believes that most of the problems in the IGF are attributable to its unique position as a bridge between the multistakeholder IG community and the United Nations system, which gives it no guaranteed budget but at the same time ties it to UN conference protocols and UN processes and politics. There is evidence that this bridge is crumbling and it's not clear it can be repaired under the current framework.

While IGF is a multistakeholder forum, it has to comply with the UN conference protocols. The UN conference protocols are designed for host countries and Nation States to protect their interests. This means that IGF through its host country has to pay for strict UN security protocol in negotiations with the local police (unless the conference is being held on a UN premise which already complies with the security protocol). While this brings immunity for the participants, it only does so within the UN premises for the duration of the event. Nationals of countries that are not a member of the United Nations cannot even register to attend the event.

The concept of no “ad hominem” attack on nation states or any other group is also sometimes arbitrarily practiced, which leads to confiscation of materials that are critical of one group or a nation state. While the no ad hominem attack rule might encourage more corporations and nation states to attend IGF, since it is arbitrarily enforced it is not very clear how it has affected the discussions.

IGF’s MAG is appointed through a highly arbitrary process with little transparency. Stakeholder groups do not get to select their own representatives in a bottom up fashion but send a list of recommendations into a UN black box and wait for some behind-the-scenes deals and criteria to produce a result. The program decisions made by the MAG have become progressively worse. It seems that the MAG as a collective entity has no coherent vision of what issues are important and who are the key people and stakeholders to bring them forward. Application processes put too much emphasis on stakeholder, geographic and gender quotas and too little emphasis on the significance of the topic and the quality of the ideas.

We encourage NTIA to support changes in the procedures for appointing MAG members and improvements in workshop review and approvals. Procedures should put selections in the hands of stakeholder groups and not in the hands of ECOSOC. We also encourage NTIA to find ways to encourage business, governments and civil society to use the IGF as a platform for real bargains and agreements around internet governance.

The private sector participation in IGF is extremely low (14-15% in 2017 and 2016). Government participation is not much better (20% in 2017 and 2016). Most of the attendees are from the civil society stakeholder group (44% in 2017 and 2016). Even when governments do participate they tend to segregate themselves in Open Forums for intergovernmental organizations, which are really one way public relations sessions and not dialogue. If we want UN sponsorship of the IGF so that governments and intergovernmental organizations can interact with other stakeholder groups, then obviously we are failing. IGF imposes burdensome UN conference protocols that make it prohibitively expensive to host and then it doesn’t even facilitate what its mandate requires it to do. We fully recognize the fact that having a UN style meeting helps the multistakeholder processes to gain recognition within intergovernmental organizations and nation states. But IGF secretariat and MAG have to use all the resources available to them to increase the interest of governments and private sector to engage seriously with all stakeholders at IGF.

IGF is, in the end, little more than a forum where Internet issues can be aired and discussed. Many other organizations and forums can and do organize conferences that meet the same need. Specific examples that come to mind are RightsCon, the GCCS series, various university and research-institute conferences, and even the ITU WSIS forum. What unique value does the IGF add? While from 2006 - 2012 or so IGF was the central convergence point for Internet governance discussions, it has become increasingly difficult to get good ideas for workshops past its Multistakeholder Advisory Group (MAG). Main sessions have for many years been dead

zones in which ridiculously large panels engage in unfocused discussions that are largely designed to be innocuous. The IGF's struggles in finding a venue for 2018, and resultant uncertainties for those planning to participate, are very damaging to its status as a leading world forum. Those responsible for IGF need to understand that people have alternatives to it and unless it adds some kind of distinctive value to global IG discussions it will be ignored.