Submission to the Global Stakeholder Meeting on the Future of Internet Governance

- Area: COMBINED INTERNET GOVERNANCE PRINCIPLES AND ROADMAP
- Entitled by: Nick Ashton-Hart
- Region: US, EU, Geneva
- Organization: Computer & Communications Industry Association (CCIA)
- Sector: Private Sector
- Keywords:

Abstract

PRINCIPLES DEVELOPMENT:A healthy and effective Internet Governance ecosystem presupposes agreement on what is, and what is not, within the scope of that term. Despite the adoption of a definition of Internet Governance almost 10 years ago, disagreement on its meaning continues. We propose four principles we believe the Meeting should endorse to create a common understanding of what aspects of policy should properly be considered as Internet governance related, principles we believe are not in conflict with the Tunis Agenda definition.ROADMAP FOR THE ECOSYSTEM:A roadmap only becomes practical if agreement on the scope of what is, and is not, Internet Governance related can be achieved. We build upon the Four Principles in this section to propose:1) A set of improvements to IG processes;2) Mechanisms for IG processes to relate to other policy areas not IG related but with an internet dimension.

Document

Submission to the Global Multistakeholder Meeting on the Future of Internet Governance

8th March 2014

Section 1. Internet Governance Principles

The Computer & Communications Industry Association (CCIA) welcomes the opportunity to participate in the Global Multistakeholder Meeting on the Future of Internet Governance ("the Meeting"). CCIA represents a broad cross-section of the world's leading technology companies that collectively employ hundreds of thousands of people and generating hundreds of billions of dollars in annual turnover, contributing to the economies of the majority of the world's countries and territories and in all its regions. Like the rest of the economy, our member companies rely on an open, stable, secure, resilient, and interoperable Internet. We believe that a healthy, vibrant, stable, effective, and pluralistic Internet governance system is essential, and that all stakeholders with a role in developing, maintaining, or using the Internet must be able to participate in, and impact, decisions that would impact them or it.

Four Principles to Create a Common Understanding of What Is, and Is Not, Internet Governance-Related

In order to have a healthy and effective Internet Governance ecosystem, it is first necessary to have agreement on what is, and what is not, within the scope of that term. Despite the adoption of a definition of Internet Governance almost 10 years ago[1], disagreement on its meaning continues to this day.

We propose four principles we believe the Global Stakeholder Meeting on the Future of Internet Governance should endorse to create a common understanding of what aspects of policy should properly be considered as Internet governance related, principles we believe are not in conflict with the Tunis Agenda definition.

First Principle: The network and the data that network carries are in fact (and are to be treated as) entirely separate at the policy level

The "network of networks" that is the Internet is made possible by a set of systems and services that interoperate to make it possible for any point "a" to connect to any point "b" anywhere in the world. These systems and services operate separately from the data that is communicated once the connection between points is made. It consists of: unique identifiers like Internet Protocol (IP) addresses and Domain Names; submarine, overland cable, satellite and mobile links; Internet exchange points (IXP); and software and hardware based security infrastructure implementing common standards (such as DNSSec) to ensure the point 'b' you reach is the *authentic* 'point b'.

Second Principle: No stakeholder may take measures that compromise the ability of the network to connect the greatest number of users at the lowest cost and as efficiently as possible.

We note that a subset of this is that countries must not take measures with respect to the network infrastructure located on territory under their control that would impact neighbouring or other countries to which that infrastructure directly connects - just as countries are constrained, for example, from disruption to riverine systems that pass through multiple countries other than their own.

Third Principle: The management of, and access to, data that traverses the network is not a subject of international Internet Governance.

The understanding of what constitutes private information, criminal behaviour, libel, fraud, and many other aspects of communications are the remit of national law; defining these terms is an essential element of national sovereignty. Where international law addresses issues to create global norms or processes, those fora are best suited to discuss and reach agreement on measures for the digital environment *as regards data in that domain*. In other words, what takes place online is no different than what takes place in the physical world. Both spheres tackle the same challenges and the existing mechanisms for dealing with those challenges should be utilized rather than create a separate set of organizations or rules that only apply to the Internet. For example, with respect to human rights, the Human Rights Council and the instruments to which it relates address the online and offline aspects of that area of law. With respect to the economic use of data, there are international arrangements and processes in world trade law such as the WTO, UNCTAD, and OECD (for all, developing, and developed countries respectively) whereby commercial rules between countries as well as bilateral arrangements are dealt with.

Fourth Principle: Regulating the Internet, or technology more generally, will not solve social problems.

The surveillance activities revealed over the last several months that are the subject of concern are spawning proposals in various countries, such as obliging commercial

operators to host certain kinds of data in given geographic locations. This will have unintended negative side effects without changing the relative security of that data, and without solving the underlying issue related to the lack of cooperative arrangements between countries to ensure governments can ensure the security of their citizens. Such a discussion is fundamentally not about the Internet or Internet Governance but rather how all stakeholders can cooperate regarding serious security threats.

A general agreement on the above four principles would bring a great deal of clarity as to what is, and is not, the proper remit for activities related to Internet Governance and where subjects with an 'Internet dimension' that are not Internet Governance related should be discussed. It would also make designing and delimiting Internet Governance activities more sustainable, likely to result in discussions with maximum utility, and ensure outcomes with the least likelihood of unintended negative consequences.

Global Internet Governance principles

As noted above, there already exists a fulsome list of global principles that apply to the Internet. The compilation of Internet Governance principles on the NetMundial website is quite exhaustive and reflects a broad international consensus. In particular, we draw attention to the Internet Governance Principles by the Council of Europe, the EU Commission COMPACT, the Principles for the Governance and Use of the Internet by CGI.br, the OECD Principles for Internet Decision-Making, the Global Network Initiative Principles, and the APC Code of Practice on Internet Governance, which all offer very balanced and sensible guidelines.

We believe that NetMundial could serve a very valuable purpose by seeking to distil those principles into a set generally agreeable across all stakeholder groups. From our perspective, the following principles seem of particular value to define what Internet Governance processes should embody:

? Inclusiveness and diversity

? Transparency and accountability

? Access

? Universality

? Interoperability and Standardisation

? Security, stability, and decentralization of the network

? Openness and neutrality of the network

With respect to multi stakeholder participation, we suggest there is a need to adopt a set of minimum standards for the quality and nature of such participation, and that this should be based upon existing understandings such as the Aarhus Convention's commitments on public participation and the process of broadening that understanding beyond the Convention's remit.[2] The International Association for Public Participation (IAP2) has also done excellent work in this vein; its Core Principles are widely used[3].

Section 2. Roadmap for the Further Evolution of the Internet Governance Ecosystem

Introduction

To create a road map for Internet Governance going forward, a common understanding on what is, and is not, within scope is necessary; taking the four principles above as a foundation, we have proposals below on how to improve Internet Governance arrangements.

However, the question of how Internet Governance arrangements intersect and interact with other public policy issues that have a strong 'Internet dimension' is equally important. This was anticipated 10 years ago in the Tunis Agenda's Article 35(a):

"Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues."

Like the definition of Internet Governance itself, this paragraph has also been subject to disputed interpretation. We suggest some ideas for how Internet Governance processes can better relate to these policy areas, when appropriate, below.

Roadmap for Core Internet Governance Issues

If you accept the four principles developed in section 1, it becomes much simpler to identify core Internet Governance issues.

Internet protocols and other technical standards have rapidly evolved through a set of diverse organizations, each with different core functions and strengths. In our view, and as other submissions have pointed out, stakeholders should continue to rely on the existing structures to develop global policies and seek to improve them where necessary rather than relying on either existing multilateral arrangements or starting over and creating a new governance body with a duplicative function.

Existing Internet Governance arrangements include institutions like the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and the Internet Architecture Board (IAB) for global standards and protocols, the Internet Corporation for the Assignment of Names and Numbers (ICANN) and Regional Internet Registries (RIRs) for the coordination of unique identifiers, and the UN's Internet Governance Forum (IGF), which brings together all stakeholders including academia, governments, civil society, and industry to foster discussion or critical Internet issues.

What these arrangements share is an understanding that all stakeholders who have a role in developing, maintaining, or use of the Internet must be able to participate in, and impact, decisions that would impact them or it. There are many perspectives on multi-stakeholder-ism and what it means. The reality is that the Internet of today is a web of collaboration, built upon open standards, involving all the parties necessary to ensure the Internet and the data it carries operates today and evolves for tomorrow.

Here are just a few ideas for how existing organisations could be improved:

? *Increased outreach, capacity building and training for regulators.* While many if not all of the technical meetings are open to all participants, the majority of the meetings historically have taken place in the developed world and their processes can be difficult to grasp as a newcomer. We applaud recent efforts undertaken by the IETF and ISOC to increase the global reach of their meetings as well as offer fellowships to engineers and

policymakers from the developing world. We would support similar efforts in this space in other fora as these present important opportunities to engage thought leaders globally.

? *Increase and diversify newcomer sessions*. International organizations should make it easier for newer participants to meaningfully engage in their processes. To do this, these organizations should offer training and newcomer sessions both at their physical meetings and remotely as a means of introducing more people to the organizations and encouraging them to participate in critical Internet governance debates.

? *Improve transparency and accountability*. Multilateral organizations whose missions touch the Internet (e.g., UNESCO, OECD, UN, and ITU) should provide better transparency and accountability in their decision-making processes and how the overall decisions impact the Internet. All institutions should strive to make relevant governance and policy documents available to all stakeholders at no cost - and easy to find.

? *Open, accessible meetings.* Participation in board and governance meetings of Internet governance organizations should be open whenever possible. For many participants, it is difficult and often cost-prohibitive to attend meetings in person. For that reason, Internet governance institutions should improve remote participation logistics and opportunities.

? *Improve accessibility of institutions and reduce barriers to entry*. The assortment of organizations and overlapping missions can be confusing and difficult to navigate without considerable time and effort. All institutions should collaborate to create portals online where their interrelationships and the scope of their activities is easy for new entrants to understand.

? *Institutions should consider collaborating to organize physical meetings of more than one organisation in the same city and closely enough in time that participants could attend them all; this would reduce travel costs and time*.

? *All organisations with a global mandate have an obligation to ensure multilingual documents and interpretation in multiple languages is available for key documents and meetings respectively.*

Policy Areas With an Internet Dimension But Outside of Internet Governance

What about issues that are not covered by these policy fora? We submit that they fall into two categories or types:

1. Issues where international norms exist, but where a networked world has created challenges in implementation of these norms;

2. Issues where no norms exist but where conflicts in national laws have arisen primarily because of a networked world.

Both fall squarely within the Fourth Principle's ambit: they are social issues with an online component but they are not Internet issues – and therefore entirely outside Internet Governance. Here are examples of each:

Type 1

Human and Political Rights: The various human rights treaties are the responsibility of the UN's Human Rights Council (HRC) and some of the provisions are considered *jus cogens*

- globally binding on all States. The HRC has decided that existing human rights apply fully in the online environment. However, many states are facing difficult questions: how does the right of free speech apply within their states when non-nationals may post information to non-locally-based, yet locally-used, popular websites that infringe local laws or social mores.

Type 2:

The treatment of personally identifying information (PII) falls into two categories:

1. Its use by non-state actors, and;

2. Its use by state actors.

In neither case are there international norms specifically addressing the use of PII[4]. This is because in an analogue past, physical data related to people simply didn't travel across borders routinely in large amounts related to entire populations, yet on the Internet this happens daily and routinely. It must be emphasised that these two categories are entirely different in almost every respect and need to be dealt with separately for a multitude of reasons, just the most stark example being that use by non-state actors generally involves consent by the user, and use by state actors not only is often non-consensual but is often not even known of by the user.

Roadmap for Policy Areas With an Internet Dimension

For issues of 'Type 1' there's a need for the 'Internet dimension' to be fully a part of the deliberations of those processes mandated to address them. Creating additional

processes that are ‘Internet-centric’ to address them would be a mistake:

1. The subject matter is not fundamentally Internet related and so shouldn’t ‘belong’ to Internet policy;

2. The subject matter expertise is centred in the existing process and decisions made without that context and expertise are unlikely to be as well-informed as they should.

Existing fora need to accept that the Internet dimension to ‘their’ issue must engage all stakeholders in developing solutions that they will either need to live with or help implement. This requires a truly multi-stakeholder process to bring the Internet community into collaboration with existing processes that are not inherently multi stakeholder (such as the UN’s HRC). Such processes should be based on existing best practices and norms as previously mentioned.

With respect to Type 2, the challenge is more complex. First agreement that an international discussion on the subject is needed, and further agreement on what aspects of which of the two subtypes mentioned above should be discussed and in what context. For example, the treatment of non-nationals by national security mechanisms are greatly complicated because the Internet allows the gathering of information globally at a low marginal cost and almost instantly yet the only norms that are not contested by states to limit their behaviour are bilateral agreements such as Mutual Legal Assistance Treaties (MLATs)[5], most of which predate the Internet’s widespread adoption.

How Can Internet Governance Policy Interact with Issues that Impact the Internet, Yet Are Outside the Scope of Internet Governance?

In many ways, the Global Multistakeholder Meeting on the Future of Internet Governance is an attempt to answer the question immediately above: without the surveillance disclosures of the last several months, the Meeting would not have been proposed or convened. A dynamic has been created where governments feel action must be taken to protect their citizens' data from foreign surveillance agencies. One avenue they're clearly pursuing is to look at Internet Governance arrangements due to the historical accident that has provided a unique role to the US government with respect to certain technical functions.

A major success for the Meeting would be to create a consensus around the ideas we espouse in the Fourth Principle and then through proposing practical measures that can meet the gap in the current landscape.

One of the most straightforward is through improvements to the Internet Governance Forum system (the international IGF and the regional and national versions). All stakeholders are represented in these meetings, yet the discussions too often do not have conclusions; where they do, there is no mechanism by which those conclusions can be taken further. We suggest the following:

? The IGF should continue to be an informal, dialogue-centred process, but that dialogue should prioritize the activities that fall into two main areas, rather than continuing to simply host workshops in various subject areas as has been the case thus far:

a. Look at the various areas outside Internet Governance where a profound impact on the Internet, or where Internet Governance could have a profound impact, is likely and the venues where those areas are being discussed and create opportunities for the IG community and those other communities to interact. The IGF should also seek to identify issues with an Internet dimension that are not currently being addressed elsewhere and consider how a conversation could be structured as a starting point, if there's general consensus that such a conversation is needed;

b. Create space whereby the national and regional IGF conclusions are visible and discussed at the international IGF, and vice-versa, to allow better sharing between these IGFs of good ideas, concerns, and activities.

? The IGF Secretariat should be greatly strengthened and mandated to create interagency links between existing fora where the Internet dimension is identified by the IGF as significant; it should also be able to propose processes that need attention to the IGF. It should also have the capacity to track and interact with discussions with an Internet dimension taking place in other agencies or processes and create dialogue between it, the IGF, and those others.

Conclusion

In order to develop a common understanding of, and a road map for the future development of the global Internet policy landscape, it is fundamental to establish a clear distinction between core Internet Governance issues and the wider set of issues with an Internet dimension.

While it is important to make existing Internet Governance arrangements more diverse and accessible, the key question is how they are to interact with other policy areas outside of Internet Governance, but with an Internet dimension. This includes both areas where international norms exist, i.e. through Human Rights obligations, and areas that are fundamentally governed by national laws and where no international norms exist, i.e. the use of PII information.

Instead of creating additional, ‘Internet-specific’’ processes to address areas where the subject matter is not fundamentally Internet related and the expertise is, therefore, centred in other, existing processes, existing fora need to embrace the Internet dimension of their issues and start to engage with the Internet community. With regards to the latter, the

situation is more challenging. Before effective international coordination can take place, agreement on the need for norms need to be reached - or at least the need for an international ‘conversation’.

The IGF should play a key role. It can facilitate the coordination between existing institutions and the Internet community and it can help identify new areas where international norms are needed. However, the IGF and its Secretariat would need to be strengthened to assume these additional responsibilities.

We thank the organisers of the Meeting for this opportunity to submit our views and look forward to the next steps and to the meeting itself.

[1] Tunis Agenda for the Information Society, Article 34, at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[2] The relevant text of the Convention may be found here: http://www.unece.org/env/pp/contentpp.html while more information on the process of expanding and implementing these principles is here: http://www.unece.org/env/pp/ppif.html

[3] The Core Values of IAP2 are to be found here: http://www.iap2.org/?page=A4

[4] Though it is certainly true that human rights instruments affirm a right to privacy, these obligations are not granular enough to define what activities may be undertaken by what stakeholders and in what circumstances and states have not, so far, been able to reach consensus on the relationship between these obligations and national security in the online environment in key respects.

[5] AccessNow has created an excellent website with material about MLATs worldwide in the context of access to PII of individuals. It can be found at https://mlat.info/app.php/.