Internet Architecture Board (IAB) response to the NTIA Notice of Inquiry

July 16, 2018

The Internet Architecture Board (IAB) provides long-range technical direction for Internet development, ensuring the Internet continues to grow and evolve as a platform for global communication and innovation. It also provides oversight of a number of administrative activities and relationships on behalf of the IETF, including the IANA relationship with the IETF. The IAB is chartered both as a committee of the IETF and an advisory body of the Internet Society. Further details about the IAB are documented in RFC 2850 <https://www.rfc-editor.org/rfc/rfc2850.txt>.

The IETF is a global organization whose goal is to make the Internet work better. The IETF is responsible for the key technology standards that are used on the Internet, including IP, TCP, DNS, BGP, TLS, and HTTP, to name but a few. IETF standards are published in the RFC series. For further information about the purpose and mission of the IETF, see RFC 3935, "A Mission Statement for the IETF" <https://www.rfc-editor.org/rfc/rfc3935.txt>.

The IAB thanks the NTIA for requesting feedback and guidance from the Internet community regarding policy priorities.

IANA Transition

Section II, Question D of the NOI asks "Should the IANA Stewardship Transition be unwound? If yes, why and how? If not, why not?" This question is the one that affects us most directly, so we treat it first and then offer our thoughts in response to some of the other questions in what follows. In short, our answer is no.

For context, the IETF, the Regional Internet Registries (RIRs), and ICANN are the three direct customers of the registry services provided by the current IANA operator. IANA registries hold information about IETF protocols relating to protocol parameters such as port numbers. IANA registers and maintains protocol parameters based on IETF consensus decisions and requests from individual developers in the Internet community. As a result, the IETF depends on the correct operation and appropriate organization of the IANA Functions. In our view, while IANA serves a useful registry function, it is not a governance function as such, but a basically clerical function. IANA maintains a public record that fosters interoperability by ensuring that the Internet community shares a single view of these parameters.

The IAB provides oversight to the maintenance of the IETF protocol parameters, is responsible for selecting appropriate parameter registry operator(s), and is responsible for arrangements for each registry.

One additional entity, the IETF Trust, also plays an important role in the organisation of IANA Functions. The IETF Trust is registered in the Commonwealth of Virginia. Among other responsibilities, the IETF Trust owns intellectual property rights associated with the IANA Functions. These property rights include trademarks and domain names. For instance, the domain iana.org is registered to the IETF Trust.

Our answer to the NTIA's question is that the IANA Stewardship Transition should not and, for practical purposes, cannot be unwound. It would be like an attempt to un-pop a balloon.

To begin with, and most importantly, the post-transition system is working well for the Internet. The process of preparing and completing the transition took a large number of participants multiple years to complete. These participants proceeded with the transition with all due care. The conditions that have prevailed since the transition illustrate how well they did: nobody noticed. It worked. It is not in any way desirable to change something that is working so well without a very strong reason.

The IETF and the IAB monitor the IANA arrangements and their performance closely (see, for instance, https://www.iana.org/performance/ietf-statistics). There are also yearly audits (see https://iaoc.ietf.org/reports.html). The IANA operator performance remains outstanding, both before and after the transition.

The current arrangements took time and effort to set up. The many parties who were involved devoted that time and effort to make it happen because they believed that the result would be positive for the Internet. But there is no reason to suppose that an attempt to undo that work would result in the same level of voluntary cooperation. Rather, it is likely that there would be no cooperation at all. In that event, the effort to unwind the transition would require undoing both formal contractual relationships and non-contractual processes within the affected communities, and the reconstruction of the previous arrangements, but without the cooperation of the affected parties.

In the event the previous regime were in fact restored, it is an open question as to whether the Internet would continue to use IANA as its means of coordinating these registries. Since the Internet is voluntary, everyone could simply adopt a new means for coordination. More likely, many different factions would attempt to stake a claim on some of the IANA registries, producing confusion and splintering of the Internet.

In addition, as part of the transition, ICANN transferred certain intellectual property (e.g. the domain name iana.org and the trademarks related to IANA) to the IETF Trust, which is organized under the laws of the Commonwealth of Virginia. While it is certainly logically

possible to transfer the intellectual property back to ICANN, the current terms of the IETF Trust Agreement forbid this action.

In short, an attempt to reverse the IANA Stewardship Transition would break a working system for no apparent benefit, at the cost of a great deal of work, and would be against our wishes as one of the affected parties. More broadly, attempting to unwind the transition might result in the breakdown of the IANA system or the splintering of the Internet. This would likely damage global Internet businesses, including those residing in the United States. In other words, it poses significant risk without prospect of any reward. It should not be undertaken.

Other Matters

I. The Free Flow of Information and Jurisdiction

Section I, Question E. What should be the role of all stakeholders globally—governments, companies, technical experts, civil society and end users—in ensuring free expression online?

We believe that the freedom of expression includes the freedom to create content, services, and even new technology. This free flow of information is central to the Internet ecosystem's architecture, to its ability to flourish, and to the ability of its participants to innovate.

The Internet is a complex system, and changes in one aspect often have impacts elsewhere. Matters that appear simple when considered by one stakeholder often have surprising effects when considered by other stakeholders. As a result, it is crucial that any significant changes are carefully vetted in a broad discussion that includes a wide range of input from technical (including software, equipment manufacturing, and network operations) and other stakeholders including academic, civil society, public policy, and user expertise. This is not just an accidental property of the way the online world works. Because the Internet is made up of many independently operated networks, such coordination is the only way that a given change can be implemented is by all affected parties. The best way to get such implementation is to ensure that all the affected parties are involved in working out the desirable path for change.

Any party wishing to see particular objectives fulfilled may not be able to operate in this environment simply by making changes on their own or by requesting or ordering others to make change. Collaborative approaches for change work better. One good role for governments is that of facilitator, ensuring that the key participants in the Internet ecosystem are involved in any effort to drive change.

II. Multistakeholder Approach to Internet Governance

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

The IAB believes that the multistakeholder approach continues to be the only viable approach to have such an environment. That is how the Internet works. As discussed earlier in this response, many Internet activities depend critically on multiple cooperating parties and on their motivation to continue that cooperation.

For instance, the development of new technology typically requires the participation of those willing to develop the technology and build systems or software, with those who operate the systems, along with security researchers who can analyse the system. And in some cases, policy or business expertise is necessary as well.

It is difficult to imagine a workable model other than the multistakeholder one. This is largely because the Internet has no centralized control. Networks connect to the Internet because they see benefit in doing so. Software developers produce features and systems that benefit their users and business interests. Yet, many Internet issues that require coordination, such as IP address allocation, need broad if not universal acceptance of decisions for the Internet to function properly. It is unlikely that any top-down hierarchical or multilateral system, for instance, could work. Cooperation in the Internet typically works in another direction, that is, bottom-up or peers working together to achieve something.

But perhaps most importantly, the Internet has proven to work on the multistakeholder model for more than 30 years, and continues to grow and generate new innovations at a fast pace. Those who would replace it with some other model would need compelling justification that an alternative model would be likely to command the global acceptance and support that the multistakeholder system does. Without such justification, parties will simply refuse to cooperate, and without cooperation the Internet would likely fragment, eliminating many benefits for all stakeholders, especially the Internet users.

Section II, Question 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?

Different topics require different levels of coordination. For instance, the allocation of IP addresses has to be done in a manner where everyone has the same understanding of what addresses have been allocated and where, and what address space is usable for allocations. This requires coordination among the IETF that defines the address ranges, the RIRs, their communities, and broader discussions of policies at global, regional, and local level. This is one topic that is extremely suitable for a multistakeholder approach.

Some other topics may require less coordination. For instance, the details of a particular technology may not matter to much beyond the implementers of that technology. Here the set of parties needing to collaborate is smaller, perhaps just the implementers and their target users and security experts.

Still other systems can be deployed on the Internet without any coordination at all. For instance, many modern web-based services and applications (whether apps on a mobile device or services such as Facebook or Twitter that are delivered in a general-purpose web browser) do not really require coordination with anybody else for them to work well. These all depend on standard protocols, such as HTTPS, like any other web page, but otherwise require no additional coordination with anyone.

Not every service that is delivered over the Internet is really strictly a *part of* the Internet, and such services are often areas of public interest where other mechanisms than the multistakeholder approach works. For instance, credit card transactions handled on the Internet have policies that, while admittedly developed by multiple stakeholders, can be better thought of as "industry self-regulation" or "regulation-driven codes of conduct" than as "multistakeholder".

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

We believe that the existing accountability structures are indeed sufficient.

To begin with, there is an important, practical sense in which accountability structures for Internet governance bodies are sufficient by definition. Because the Internet only works if networks voluntarily interconnect and operate together, any system that is insufficient to keep that working properly will be ignored by the participating networks, and be replaced by something that is sufficient to the independent operators' preferences. The system is *in essence* voluntary, so if there is an Internet at all then the system is sufficient to the needs of the participating networks.

At the same time, naturally, all systems created by humans need constant refinement towards a greater perfection. That means we can always identify parts of the system that could be improved. For instance, it can be difficult for someone unfamiliar with the history to understand the institutional relationships in some parts of Internet governance. However, because everything is fundamentally voluntary, the incentives are aligned correctly to make sure that insufficiency will be addressed as new needs arise. So, for instance, the IANA protocol parameters registries are overwhelmingly maintained through the IETF. If there were needs by Internet software developers, for instance, for different arrangements, they could easily set up new mechanisms. That we do not see this happen regularly is good evidence that the accountability of the structures actually in place is good enough for the purpose.

The IETF itself has strong accountability through its processes, and the Internet technical community is satisfied with the arrangements. IETF decision making is undertaken through rough consensus that is worked out in public on mailing lists to which anyone in the world may subscribe and contribute. The people who judge whether consensus has been reached -- the Area Directors -- are selected at regular intervals by a nominations committee (NomCom); the members of the NomCom are volunteers who are regular participants in the IETF, and who are seated by random lot. Every decision is subject to requests for reconsideration by the same bodies, and then by appeal to other bodies. Area Directors are seated for terms of two years, and they can also be recalled by the community. Further details about the design of the accountability mechanisms at the IETF can be found in RFC 7979 <https://www.rfc-editor.org/rfc/rfc7979.txt>.

In the final analysis, the voluntary nature of the Internet means that a truly illegitimate decision would be ignored by the independent network operators anyway. Everyone involved knows that, which provides significant incentive to keep the system working smoothly.

This approach, which is the one that was used both before and since the IANA stewardship transition, has been working for many years. The evidence of its success is the functioning Internet on which we depend every day. It is worth observing that a change to these arrangements would not be without cost, and anyone proposing that such changes be made bears the burden of proof to demonstrate that the changes are needed, that they would be beneficial for the Internet and its users, and that undertaking such changes is worth more than other things that the Internet community could do instead.

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

The IAB is always pleased to see the NTIA's participation in and support of multistakeholder efforts to foster stable and effective operation of the DNS.

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

The IAB believes that it is important to have fora, such as the IGF, the OECD ITAC, and regional meetings, where Internet governance topics can be discussed among all of the stakeholders, including governments. It is desirable for the IGF to facilitate multistakeholder discussions of these topics. The IAB would like to highlight the need for involvement of technology developers when policy topics are discussed, not to drive the policy decisions, but to make sure that the policies can be implemented.

Section II, Question J. What role should multilateral organizations play in internet governance?

The IAB would like to point to the 30+ year history of the Internet and the development of various mechanisms to assist in tracking those issues that require global coordination and discussion. The ecosystem that has developed throughout this history is today working well and generally on top of the topics that it needs to handle. There are roles for multilateral organisations as part of the overall system, for instance, in frequency allocations (ITU-R). But as explained earlier in this response, the voluntary and collaborative nature of Internet connectivity and interoperability requires most primary issues around the Internet to be dealt with in a collaborative fashion, and multilateral, governments-led approaches may not be the best organisation for that.

III. Privacy and Security

Section III, Question A. In what ways are cybersecurity threats harming international commerce? In what ways are the responses to those threats harming international commerce?

Cybersecurity threats have the potential to affect all online activity, not just commerce. The distinction between online and offline is largely irrelevant for both businesses and individuals.

The increase in denial of service attacks is of immediate concern across all aspects of online activity. The cost of defending against denial of service is disproportionately borne by smaller entities.

Online activity depends on encryption to defend against a range of attacks. Weakening or disabling encryption adversely affects those that rely on cryptographic defenses. This exposes those entities to new attacks, and imposes a competitive disadvantage compared to those that are not subject to the same constraints.

Attempting to control the use of encryption by filtering or blocking can have the effect of making communications between jurisdictions more difficult, which could adversely affect international commerce and other activities.

Section III, Question B. Which international venues are the most appropriate to address questions of digital privacy? What privacy issues should NTIA prioritize in those international venues?

There are a number of groups that actively discuss various aspects of online privacy. Engagement in multiple forums is likely necessary. For instance, the IETF has a number of activities around privacy in protocols, the W3C examines the impact of web technologies. Engagement with specific jurisdictions, such as the EU, might improve the consistency of legislative measures. Multistakeholder organizations can also help regulatory agencies consider the architectural or technical impacts of proposed privacy regulations.

The collection and trading of information about individuals by advertisers and large web properties is a significant problem in online privacy. Voluntary and market-based approaches have largely failed to address this problem. Attempts to control this by requiring informed consent have not been effective in altering behavior.

Large-scale collection of information about individuals by governments is another threat to privacy. RFC 7258 <https://www.rfc-editor.org/rfc/rfc7258.txt> ("Pervasive Monitoring Is an Attack") and the IAB statement on confidentiality (https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/) describe the ongoing response to pervasive surveillance.