Date: July 17, 2018

Comment from the Internet Society on the
National Telecommunications and Information Administration's

Notice of Inquiry on International Internet Policy Priorities

Docket No. 180124068-8068-01

The Internet Society (ISOC) is pleased to submit these comments in response to the United States Department of Commerce's National Telecommunications and Information Administration's (NTIA) Notice of Inquiry (NOI) on International Internet Policy Priorities[1].

The Internet Society is a global not-for profit organization committed to the open development, evolution and use of the Internet for the benefit of all people throughout the world. The Internet Society works in partnership with our global community, comprised of over 110,000 members, 136 chapters and special interest groups, and 149 organizational members. It is also the organizational home of the Internet Engineering Task Force (IETF)[2] and the Online Trust Alliance (OTA)[3].

The Multistakeholder Approach to Internet Governance

Since its early days as a research project, the development of the Internet was based on collaboration and participation by a diverse set of stakeholders. The collaborative approach that helped build the Internet is now the cornerstone for decision making in the Internet – the so-called multistakeholder approach[4]. Indeed, multistakeholder approaches to decision-making have been the foundation of the Internet's success to-date.

In recent years, the voices of countries advocating for a multilateral approach to Internet governance have become stronger, challenging the premise and functionality of the multistakeholder model, and the future of the Internet. It has been the consistent position of the Internet Society that decision-making in a complex world must be collaborative, inclusive, transparent and multi-stakeholder. In complex ecosystems like the Internet, norms need to be set by diverse communities, serving diverse needs and must be designed to be good for the whole. Processes must be flexible and decision-making must be collaborative and agile.

---

[1] National Telecommunications and Information Administration. (04 June 2018). *NTIA's Notice of Inquiry on International Internet Policy Priorities*. [Blog post]. Retrieved from: https://www.ntia.doc.gov/federal-register-notice/2018/notice-inquiry-international-internet-policy-priorities

[2] Internet Engineering Task Force: https://www.ietf.org/

[3] Online Trust Alliance: https://otalliance.org/

[4] Internet Society. (26 April 2016). *Internet Governance – Why the Multistakeholder Approach Works.* Retrieved from: https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

As voices around the world calling for greater control become emboldened, it is more important than ever that we support and implement multistakeholder approaches to Internet decision making.

The multistakeholder model is a key driver for the evolution, growth, and sustainability of an open and global Internet. Like any process, the multistakeholder model has grown, changed, and strengthened along with the growth of the Internet and its stakeholders. We know, and have experienced how, diverse participation and collaboration has led to innovative and creative ways of solving complex problems, related to Internet governance. The IANA stewardship transition is an example of this innovative problem solving (see below).

At the Internet Society, we have consistently advocated that the multistakeholder model is not an end in itself but a means towards a certain end; we believe in its inherent flexibility to adapt to different issues and to be capable of capturing diverse cultural and geographical sensitivities. Working with various communities across the world, we have seen the ability of the multistakeholder model to address Internet issues ranging from privacy, to security, to the Internet of Things (IoT).

Our experience shows that governments around the world are becoming increasingly attracted to the capacity of the multistakeholder model to adapt to and deliver effective solutions to problems that are highly complex.

A few examples of effective national and regional multistakeholder processes around the world include:

- Internet Infrastructure Security Guidelines for Africa[5].
- Personal Data Protection Guidelines for Africa[6].
- The Philippine's National ICT Ecosystem Framework 2022[7].
- Canada's multistakeholder process to enhance security on the Internet of Things[8].
- NTIA's multistakeholder process, *Internet of Things (IoT) Security Upgradability and Patching*[9].

[5] Internet Society. (31 May 2017). *Internet Society and African Union Commission Launch Internet Infrastructure Security Guidelines for Africa.* [Blog post]. Retrieved from: https://www.internetsociety.org/blog/2017/05/internet-society-and-african-union-commission-launch-internet-infrastructure-security-guidelines-for-africa/

[6] Internet Sociey. (8 May 2018). *Personal Data Protection Guidelines for Africa.* [Blog post]. Retrieved from: https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/

[7] Internet Society. (9 July 2018). *Internet Society signs MoU with DICT for Strong Internet Foundation in Philippines.* Retrieved from: https://www.internetsociety.org/news/press-releases/2018/internet-society-signs-mou-with-dict-for-strong-internet-foundation-in-philippines/

[8] *Canadian Multistakeholder Process: Enhancing IoT Security*: https://iotsecurity2018.ca/

[9] The NTIA's *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching:* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

The Internet Society is calling on key governments, including the United States, to demonstrate their support for the multistakeholder approach to Internet governance. In particular, we strongly advocate for a two-pronged approach: a) governments should call for an expansion of multistakeholder consultative processes for Internet policy matters within multilateral institutions like the International Telecommunication Union (ITU); and, b) governments around the world should adopt at a national level the multistakeholder approach for all Internet policy issues in line with their commitments to the principles of the Tunis Agenda[10].

NTIA has historically been a strong advocate of the multistakeholder model and a voice for an open, secure, and globally-connected Internet. Its voice for Internet freedom is now more important than ever.

The IANA Stewardship Transition

The Internet Society believes that the IANA transition was a significant milestone in the history of Internet multistakeholder governance. The open, inclusive, and consensus-driven processes by which the IANA Stewardship Transition proposal was developed and implemented demonstrated the adaptive nature, power, and value of the multistakeholder model. The Internet community worked collaboratively to put in place the safeguards, processes, and mechanisms that have allowed the IANA functions to be managed in an open, secure, and reliable manner.

We see no reason to unwind the transition and believe that any steps in that regard would have grave consequences for the IANA system and the global Internet itself.

The work undertaken by the global Internet community from 2014-2016 to develop a robust proposal for the IANA stewardship transition demonstrated the *legitimacy* of the collaborative approach to governing critical Internet resources. It further *strengthened* the multistakeholder governance model and *enhanced* the diverse partnership and collaboration amongst the various stakeholders.

The original criteria set by NTIA[11] during the transition period have been maintained since the contract expired and the formal transition took place on September 30, 2016. More precisely, the IANA functions are currently performed by the Public Technical Identifiers (PTI) in both an *accurate* and *accountable* manner, ensuring a secure and resilient DNS and stable, accountable, and predictable management of number resources and protocol parameters, while meeting the *expectations* of the IANA customers.

[10] International Telecommunication Union. (18 November 2005). *Tunis Agenda for the Information Society.* Retrieved from: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[11] Internet Society. (29 July 2015). *Perspectives on the IANA Stewardship Transition Principles.* Retrieved from: https://www.internetsociety.org/resources/doc/2015/perspectives-on-the-iana-stewardship-transition-principles/

In fact, the Customer Standing Committee (CSC) continually rates the performance of the PTI highly, giving the organization an excellent (100 per cent) rating in six of the past 12 months[12]. Finally, the IANA transition has demonstrated the value of an *open* Internet, where transparency, participation, and access occupy a central role.

The globalization of the IANA functions was a critical step in providing additional confidence in the collaborative and inclusive Internet governance model. For the Internet Society, the smooth operation of the Internet depends upon a global, community-led, coordinated approach to managing these shared resources. The process to transition and globalize the IANA functions has been a demonstration of global multistakeholder community cooperation in action.

It is for these reasons that the Internet Society **strongly believes that the IANA transition must not be unwound. Indeed, we see no legal basis for doing so.** NTIA should stand behind the transition and continue to recognize it as a true outcome of collaboration and cooperation among different stakeholders.

The Internet Governance Forum

Since the first Internet Governance Forum (IGF) was held in Athens, Greece in 2006, it has proven to be an important venue for setting the global agenda on policy issues related to the Internet in an open and multistakeholder manner. Historically, governments, civil society, the technical community, private sector, and other interested stakeholders come together at the IGF to discuss, in an open environment, these issues together. The Internet Society has been a strong supporter of the IGF from its earliest days and believes that the Forum still has a crucial role to play in the global Internet policy dialogue.

At the same time, we recognize that, like any organization, the IGF needs to adapt to the new environments so that it remains the leading platform for global Internet governance dialogue. The Internet Society has proposed some ideas for reform of the IGF[13] and looks forward to working with others in the IGF community to strengthen the IGF for years to come.

We believe that NTIA should continue to support the IGF and to help ensure that it continues to be an important part of the global Internet governance ecosystem.

Leading by Example

The Internet Society commends NTIA on its commitment to using the multistakeholder model to identify recommendations on domestic policy issues. In particular, NTIA's 2017 multistakeholder process related to IoT Security Upgradability and Patching[14] has become a

---

[12] Customer Standing Committee (CSC): https://www.icann.org/csc#blog_updates

[13] Internet Society. (17 March 2018). Let's Reform the IGF to Ensure Its Healthy Future. [Blog post]. Retrieved from: https://www.internetsociety.org/blog/2018/03/lets-reform-igf-ensure-healthy-future/

[14] The NTIA's *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching:* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

model for other countries around the world[15]. This model, when applied to complex domestic policy issues like IoT security, is proving to provide more robust and effective solutions. Furthermore, the global nature of the Internet and the complexity of its challenge necessitates intergovernmental and global collaboration.

NTIA has an opportunity to continue its leadership by using the multistakeholder model in developing its recommendations on domestic policy issues. In addition, NTIA could also share best practices and lessons learned with their international counterparts, so that they will have the resources needed to host their own domestic multistakeholder processes.

The free flow of information and jurisdiction

Digital connectivity is one of the most significant contributors to social and economic change. The Internet is projected to connect more than five billion people by 2020. Connectivity is changing the landscape we operate in – from the way we communicate, to the way we interact with our government, to the way we do business or experience life.

The free flow of information and data is a core part of the Internet and it is the underlying cause for much of the innovation, creativity, and productivity we see taking place. This freedom has contributed to the growth of trade in digital goods, and has enabled new services to appear and old services to become more efficient. Whether it is fueling health or government services, education or employment opportunities, community building or democratic freedoms, the free flow of information is a critical factor in allowing everyone to become part of the Internet of opportunity and part of society more generally.

However, the freedom to share data and information should not be taken for granted. According to Freedom House's 2017 Freedom on the Net report[16], "2017 marked the 12th consecutive year of decline in global freedom."

It is safe to say that the decline of freedoms on the Internet – whether it relates to speech, press, or, more generally, information –has become a global trend. In this context, we see state actors deploying different ways of undermining the free flow of information, including, among others:

- A rise in Internet shutdowns[17], where state actors block access to the Internet as a whole or in part with a view to limit online communications and information sharing.

[15] In particular, the Ca*nadian Multistakeholder Process: Enhancing IoT Security* initiative is in part based on the NTIA's multistakeholder IoT security process: https://iotsecurity2018.ca/.

[16] Freedom House. (2018). *Freedom on the Net 2017.* Retrieved from: https://freedomhouse.org/report/freedom-net/freedom-net-2017

[17] Access Now. *#KeepitOn.* Retrieved from: https://www.accessnow.org/keepiton/

- A rise in technical measures to block access to content and activities considered illegal or inappropriate, with little or no due process[18].
- Criminalization and restrictions of the use of tools used for anonymous and confidential communications, such as encryption.
- Other measures creating barriers to the free flow of communications, such as user taxes on the use of social media or heavy licensing fees and requirements for bloggers.

Similarly, another trend that has emerged concerns digital protectionism or the idea of policies and rules that restrict the flow of data among countries. Such measures can make it harder for information to flow freely and can have a significant impact on economic and social growth. Digital protectionism can take a variety of forms but the most common is through forced data localization measures that raise significant security and privacy considerations.

The free flow of information and data constitutes an important component for a healthy society and a growing economy. Countries, including the United States, should ensure a consistent, predictable, human rights-based environment that facilitates and supports freedom of expression. Any restrictions should be exceptional and strictly adhere to principles of necessity, proportionality, and the rule of law. This could mean:

- Supporting technology like encryption and anonymity tools that enhance users' privacy and their ability to express freely.
- Advocating for policies that promote freedom of expression.
- Implementing laws that prohibit forced data localization schemes.
- Implementing user-friendly tools that allow users to be in control of their data. In this context, setting up solid accountability mechanisms will be key.

The United States has long been a leader of the free flow of information and it is now more important than ever that it continues to play this role in the face of a global decline in Internet freedom.

Extraterritoriality:
In its *2017 National Security Strategy*, the Trump Administration stated that ''the United States will advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services.''[19] Over the years, the number of instances where governments or courts have adopted legislation or decisions that affect users outside of their national borders has increased. While such legislation or court decisions are often well-intended, there is a risk of unintended negative consequences. Two recent examples are the

[18] The document, Internet Society Perspectives on Internet Content Blocking: An Overview, outlines the common technical approaches to content blocking, their effectiveness, who they impact and damage caused. https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[19] US Government. (18 December 2017). *National Security Strategy of the United States of America.* Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

European Union's General Data Protection Regulation[20] (GDPR) and the Supreme Court of Canada's Equustek v. Google decision[21].

Setting aside the merits of these and other well-intentioned decisions, extraterritorial actions could raise a number of concerns[22] that we believe need to be explored further:

- Setting a precedent where countries could start imposing national or regional legislation that has global impact.
- Creating unintended clashes between different laws, which could impede the roll out of global technology.
- Producing 'regulatory competition,' the notion of state actors seeking to command the international Internet regulatory environment.
- Encouraging and fostering an environment of Internet fragmentation and lack of interoperable networks and systems.

In this context, extraterritorial actions could have serious repercussions for the future of the global Internet. At the Internet Society, we believe in a global, open, interoperable, and secure Internet. We also believe in inclusive Internet governance that strives to accommodate the interests of all stakeholders globally.

The Internet Society advises that NTIA, as one of the global leaders for Internet governance, carefully evaluate the far-reaching implications of its own domestic Internet policies. The Internet's global, decentralized nature should be maintained and protected to ensure that users everywhere are able to access and benefit from the global Internet.

Privacy and security

Encryption

As a technical foundation for trust on the Internet, encryption tools support freedom of expression, commerce, privacy, and user trust, and help protect data and communications from bad actors. Encryption should be the norm for Internet traffic and data storage. Legal and technical attempts to limit the use of encryption, even if well-intentioned, will negatively impact the security of law-abiding citizens and of the Internet at large. As other countries move to limit or weaken encryption, it is crucial that the United States government refrain from weakening or limiting encryption and instead supports its use and development.

Securing the Internet of Things (IoT)

IoT is poised to transform economies and societies worldwide. The technology brings enormous opportunities, but also great risks, particularly around security and privacy. There is a need for all stakeholders, including policymakers, manufacturers, and consumers, to make good choices

[20] *The General Data Protection Regulation:* https://www.eugdpr.org/

[21] This decision requires Google to remove an entire website from its search results globally.

[22] Internet Society. (25 May 2018). *GDPR: Going Beyond Borders.* [Blog post]. Retrieved from: https://www.internetsociety.org/blog/2018/05/gdpr-going-beyond-borders/

about the future of IoT security and privacy. The *Online Trust Alliance IoT Trust Framework*[23] outlines best practices for manufacturers and developers for IoT security and privacy.

The document *IoT Security for Policymakers*[24] outlines key considerations, challenges, and recommendations for governments as they approach IoT security. The United States government should continue to support multistakeholder processes around IoT and promote the use of best practices internationally.

Conclusion

The Internet Society is grateful to NTIA for the opportunity to share our views on its Notice of Inquiry on International Internet Policy Priorities. We are encouraged by NTIA's long-standing commitment to national and global multistakeholder coordination for an open and free Internet and look forward to continuing to engage on these important issues.

[23] Online Trust Alliance. (2017). *IoT Security & Privacy Trust Framework v2.5.* Retrieved from: https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

[24] Internet Society. (2018). IoT Security for Policymakers. Retrieved from: https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/