COMMENTS OF PUBLIC KNOWLEDGE REGARDING

INTERNATIONAL INTERNET POLICY PRIORITIES

Docket No. 180124068–8068–01

Public Knowledge submits these comments in response to the National Telecommunications and Information Administration's[1] May 31, 2018 *Notice of Inquiry* regarding its international internet policy priorities in the above-referenced docket. Public Knowledge is a non-profit organization dedicated to preserving freedom of expression and an open internet. We advocate for policies that ensure universal access to affordable and open networks and that advance government transparency and the public's access to knowledge. NTIA pursues a similar mission, and we applaud the Administration's efforts to advocate on behalf of the United States for an open, interoperable internet and for a multistakeholder approach to internet governance.

The global internet faces numerous threats, ranging from governmental control and censorship to unbalanced intellectual property laws. These challenges are an

[1] ("NTIA") or ("Administration").

existential threat to internet freedom. The world needs U.S. leadership to ensure that the internet remains free and open. By engaging in multistakeholder forums such as the Internet Governance Forum ("IGF"), the United States Internet Governance Forum, and RightsCon, NTIA can learn from the concerns of global internet governance stakeholders, and shape the conversation in favor of internet openness.

The Internet Assigned Numbers Authority ("IANA") Stewardship Transition represents a proof of concept for effective multistakeholder internet governance based on accountability, transparency, and multinational coordination. Public Knowledge emphasizes that the Transition should *not* be unwound. Such a process would face substantial legal barriers and generate significant political and reputational harms to U.S. interests. NTIA should continue to take the lead in promoting the multistakeholder approach to address current and emerging threats to an open internet.

I. The Free Flow of Information and Jurisdiction

The open internet faces an existential threat as numerous challenges to the free flow of information exist around the world. These challenges are driven by the tension between a borderless world-wide internet and an increasingly protectionist, and in certain places, authoritarian global geopolitical environment. One major threat is the rise of authoritarian regimes exerting strict control over the types and quantities of information on their national networks. China, for example, has established a "Great Firewall" that only allows for information that is friendly or non-threatening to the government, even going so far as to crack down on virtual private networks that sophisticated users are employing to circumvent the government filters.[2] Online content manipulation on social media by government actors in Russia, Asia, the Middle-East, and North Africa has led to the decline of internet freedom for seven consecutive years.[3]

Differences in the understanding of what constitutes legitimate free speech, even between democracies, sometimes also limits the free flow of information. What would be free speech in the United States might be understood as a free speech violation in other consolidated liberal democracies, as it is the case with Nazi speech, forbidden in many European countries, but not forbidden in the United States. NTIA should work not to eliminate those differences, but to guarantee that information flows are as frictionless as possible between democracies with legitimate but differing views on how to best foster online discourse. NTIA should also engage bilaterally and in multilateral forums such as the Hague Conference on Private International Law to guarantee that countries don't exercise extraterritorial jurisdiction in ways that may damage the free flow of information.

The free flow of online information is also threatened by misguided data localization policies. The rise of protectionist localization policies threatens to balkanize the internet into a collection of national networks, which could undermine security and impose economic costs from data transfer restrictions.[4] While the concerns motivating

[2] *See* Jack Goldsmith, *The Failure of Internet Freedom*, Knight First Amendment Institute at 11 (2018), https://knightcolumbia.org/content/failure-internet-freedom.

[3] *See* Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy* at 1, 22-23 (2017), https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf.

[4] *See generally* Erica Fraser, *Datalocalization and the Balkanization of the Internet*, 13 Scripted 359 (Dec. 2013), https://script-ed.org/wp-content/uploads/2016/12/13-3-fraser.pdf; Josephine Wolff, *Borders in the Cloud*, Slate (Nov. 20, 2017), http://www.slate.com/articles/technology/future_tense/2017/11/countries_are_increasingly_imposing_borders_on_the_cloud.html.

these policies may be legitimate, "pushing localization for short-term social, political and economic gains could ultimately harm users and innovators."[5] Some governments implement data localization policies not with economic protectionism in mind but with a misguided but good faith desire to guarantee law enforcement access to data collected by internet companies or to protect the privacy of their citizens. Better mechanisms that do not require data localization exist for those purposes, such as Mutual Legal Assistance Treaties for law enforcement and cross-border data protection arrangements such as the APEC Cross Border Privacy Rules and Privacy Shield. NTIA should seek to promote policies that enable foreign states to pursue legitimate policies without unduly harming the free flow of information and without imposing misguided data localization requirements.

Embedding intellectual property laws into free trade agreements without limiting secondary and intermediary liability further erodes freedom online by interfering with consumers' ability to connect directly with businesses and other users through online service providers.[6] Such limitations on consumer choice also generate economic harms. For example, angel investment – an important driver for innovation and economic

[5] Jyoti Panday, *Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms*, Electronic Frontier Foundation (Aug. 14, 2017), https://www.eff.org/deeplinks/2017/08/rising-demands-data-localization-response-weak-data-protection-mechanisms.

[6] *See* Jennifer M. Urban, *RE: Empirical Research Submission for Section 512 Study: Request for Additional Comments, 81 Fed. Reg. 78,636*, 114 (Nov. 8, 2016*)* ("The proliferation of services both personal and enterprise-level—website hosting, email services, blogs, social networking, fan sites, photo and video platforms, distributed "cloud" storage and computation, and many others—appears to be possible because of the safe harbor from secondary copyright liability that section 512 provides.").

growth – is dramatically curtailed by increasing liability for content providers and holding intermediaries liable for their users' content.[7]

Users, innovators, and the open internet are all best protected by employing a transparent, multistakeholder approach to address the threats that certain data localization and intellectual property policies are seeking to meet. NTIA can play a role in helping to address these challenges by ensuring that the U.S. keeps leading the open internet by example. This includes engaging in multistakeholder forums and initiatives to advance rules that enable an open internet such as the IGF and RightsCon. The U.S. international commitments to the IANA transition and national commitment to a free and open internet serve as examples to guide NTIA's work.

II. Multistakeholder Approach to Internet Governance

When stakeholders come together to engage in transparent and consensus-based internet governance, they help preserve the open and decentralized nature of the internet that enables robust online expression. The IANA Stewardship Transition is a validation of the multistakeholder approach to internet governance. The Transition should not be unwound. Not only would such a process face significant legal hurdles, but any attempts by the U.S. to bring domain name system ("DNS") management under government control would likely lead to the end of the open internet.

As a threshold matter, privatizing IANA stewardship and putting it into international hands was a goal of U.S. internet policy from its outset.[8] NTIA's 1998

[7] *See* Comments of Public Knowledge Regarding Negotiating Objectives for NAFTA Modernization, Docket No. USTR-2017-0006 at 4 (June 12, 2017), https://www.publicknowledge.org/documents/public-knowledge-nafta-comments.

[8] *See* National Telecommunications and Information Administration, *Management of Internet Names and Addresses*, Docket No. 980212036-8146-02 Fed. Reg., Vol. 63, No. 111, 31741, 31744 (June 10, 1998) ("The U.S.

Statement of Policy regarding the management of internet names and addresses, which led to the creation of the Internet Corporation for Assigned Names and Numbers ("ICANN"), noted that the U.S. Government considered the internet to be a global medium and that, "its technical management should fully reflect the global diversity of Internet users."[9] The U.S. sought to ensure that DNS management was undertaken with international input: "In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management."[10]

The multistakeholder process of the IANA Transition has proven that this inclusive and participatory approach is the right mechanism for internet governance. The process has not been seamless. Delays in the Transition have invited criticisms that the U.S. oversight of the DNS root zone amounts to de facto control over the internet's functions.[11] Nevertheless, the multistakeholder process has prevailed. The Transition proposal, which was approved by NTIA,[12] was the result of a coordinated effort by diverse stakeholders including businesses, governments, civil society

Government is committed to a transition that will allow the private sector to take leadership for DNS management."), https://www.gpo.gov/fdsys/pkg/FR-1998-06-10/pdf/98-15392.pdf.

[9] *Id.* at 31748.

[10] *Id.*

[11] *See*, *e.g.*, Internet Governance Project, *Political Oversight of ICANN: A Briefing for the WSIS Summit*, 5 (Nov. 1, 2005), https://www.internetgovernance.org/wp-content/uploads/political-oversight.pdf.

[12] *See* National Telecommunications and Information Administration, *IANA Stewardship Transition Proposal Assessment Report*, (June 9, 2016), https://www.ntia.doc.gov/files/ntia/publications/iana_stewardship_transition_assessment_report.pdf.

organizations, and others from throughout the world.[13] It demonstrates conclusively that a bottom-up and transparent global effort to governance is possible.

In any event, potential legal challenges make unwinding the Transition impractical. U.S. involvement in ICANN was governed by private contracts that have been terminated and replaced with a contract that precludes U.S. control over DNS governance.[14] Any efforts by Congress or the U.S. government to wrest back control over the DNS root zone would be seen a first step in the nationalization of the internet and would provide the governments that were concerned about the U.S. role in ICANN with evidence that their concerns were well-founded. It is no exaggeration to say that this would endanger the open internet as we know it as governments around the world mobilize to create a fractured internet of national networks.

To preserve an open internet and the free flow of information, this outcome must be avoided at all costs. The Transition enjoys broad cross-sector support from industry, government, and civil society.[15] Any existing concerns are minimal due to the checks and balances on state influence in the domain naming process that currently exist within IANA.[16] To the extent that there are concerns, NTIA can play the role of ensuring that IANA's DNS governance promotes the principles of global governance and freedom of

[13] *See Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community*, IANA Stewardship Transition Coordination Group (ICG), 7 (Mar. 2016), https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf.

[14] *See* ICANN, *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*, icann.org (Oct. 1, 2016), https://www.icann.org/news/announcement-2016-10-01-en.

[15] *See Statements in Support of the IANA Stewardship Transition*, ICANN Board of Directors (Sep. 13, 2016), https://www.icann.org/en/system/files/files/iana-stewardship-support-statements-13sep16-en.pdf; *see also* Access Now et al., *Civil Society Statement of Support for IANA Transition* (May 23, 2016), https://www.accessnow.org/cms/assets/uploads/2016/05/CSstatementonIANAtransitionMay2016-1.pdf.

[16] *See* Eileen Yu, *ICANN still under US laws, but checks in place to avoid hostile takeover*, ZDNet (Jan. 19, 2016, 8:14 AM), https://www.zdnet.com/article/icann-still-under-us-laws-wont-go-under-un-purview/.

expression, advocating against the trend towards internet nationalization. Showing a continued commitment to the IANA transition and to a multistakeholder global governance of ICANN is a necessary component of any strategy to fight internet nationalization. In addition, NTIA can and should use its participation in the International Telecommunication Union, particularly in the upcoming Plenipotentiary Conference, to defend the U.S. model of internet governance showing the IANA transition as evidence of the U.S. commitment with a multi-stakeholder governance of an open internet. NTIA should continue leveraging the knowledge of the multi-stakeholder Digital Economy Board of Advisors for its mission.

III. Multistakeholder Approach to Cybersecurity

A free and open internet requires a commitment to cybersecurity, particularly in the emerging Internet of Things. The multistakeholder approach has proven its worth here as well, through programs like the National Institute for Standards and Technology's Cybersecurity Framework, the ISO 27001 standard, and the NTIA-coordinated effort to produce the Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats. These projects recognize that cybersecurity issues like automated, distributed attacks are an ecosystem-wide challenge, and can only be addressed through a multistakeholder effort.[17]

NTIA should continue to engage with other U.S. agencies and international partners in developing frameworks to address cybersecurity issues. Any policy effort to

[17] *See Report to the President on Enhancing Resilience Against Botnets*, U.S. Dep'ts of Commerce & Homeland Sec. (May 22, 2018), https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

improve cybersecurity will require broad commitment from a variety of stakeholders in order to have a meaningful impact. The traditional approach has confined the discussion of national strategies largely to the military and intelligence communities, which are secretive by design, and focused more on security than on protecting privacy and free association.[18] A more effective approach calls for engaging the industry leaders who own the networks, edge-service providers, device manufacturers, policy advocates, and educational networks to balance equities and empower the public.[19] This type of multistakeholderism encourages transparency, which is needed to overcome the current environment of fear, uncertainty, and doubt (FUD) bred by the traditional approach. FUD has proven to be useful at raising awareness about the existence of a threat, but bad at breeding solutions or improving behavior in the ecosystem.[20] Further, transparent processes which engage the private sector will help to combat efforts by authoritarian regimes and others that use cybersecurity as a cloak to content moderation, widespread surveillance, and other actions that counter human rights. A multistakeholder approach will also ensure that network owners and edge providers have a voice in regulatory efforts, helping to mitigate potential negative impacts to international commerce.

[18] *See* Marília Maciel, Nathalia Foditsch, Luca Belli and Nicolas Castellon,Fundação Getúlio Vargas, *Cybersecurity, Privacy and Trust: Trends*, Fundação Getúlio Vargas, *in Latin America*, *in Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report*, Observatory Cybersecurity in Latin America and the Caribbean (2016), https://publications.iadb.org/bitstream/handle/11319/7449/Cybersecurity-Are-We-Prepared-in-Latin-America-and-Caribbean.pdf?sequence=1&isAllowed=y.

[19] *See, e.g.*, Hans de Bruijn & Marijn Janssen, *Building Cybersecurity Awareness: The need for evidence-based framing strategies*, 34 Gov't Info. Quarterly 1 (Jan. 2017), https://www.sciencedirect.com/science/article/pii/S0740624X17300540; *Cybersecrity Program Should Be More Transparent, Protect Privacy*, Center for Democracy & Tech. (Mar. 30, 2009), https://cdt.org/insight/cybersecurity-program-should-be-more-transparent-protect-privacy/.

[20] Sam Curry, *Cut the FUD: Why Fear, Uncertainty, and Doubt is harming the security industry*, Helpnetsecurity (Nov. 29, 2017), https://www.helpnetsecurity.com/2017/11/29/fud-cybersecurity/.

IV. Conclusion

We encourage NTIA to continue its long-established and carefully-considered approach to internet governance. Thanks in large part to NTIA, the U.S. Government is a leading champion of a borderless and open internet and a multistakeholder model of governance. In the present geopolitical context, where many around the globe question the values of openness, the free flow of information, and participatory structures, it is critical that the U.S. continues to lead those who believe that the value and strength of the internet resides precisely in the fact that no one owns it. We emphatically believe that the IANA transition illustrates the success of U.S. commitment to an open and free internet. The IANA transition should not be unwound.

Respectfully Submitted,

Gus Rossi
Dylan Gilbert
Mark Peterson

Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

July 17, 2018