



R. Edward Price
Senior Counsel
International Regulatory Affairs
200 Meridian Centre Boulevard
Suite 130
Rochester, NY 14618
Tel: 585.255.1227
ted.price@centurylink.com

July 17, 2018

Via Email — iipp2018@ntia.doc.gov

Ms. Fiona Alexander
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4706
Washington, DC 20230

**Re: NTIA Request for Public Comments on International Internet Policy
Priorities for 2018 and Beyond, Docket No. 180124068-8068-01**

Dear Ms. Alexander:

CenturyLink submits these comments in response to the National Telecommunications and Information Administration's ("NTIA's") Notice of Inquiry dated May 31, 2018, in the above-referenced docket ("NOI").¹ We commend NTIA for initiating this proceeding because continued growth and innovation in the global Internet-enabled economy depends on creative and forward-thinking resolutions of the issues raised in the NOI, primarily through international multi-stakeholder processes. The U.S. business community is a key partner in this endeavor.

CenturyLink is keenly interested in the issues raised in the NOI. With customers in more than 60 countries and an intense focus on customer experience and satisfaction, CenturyLink strives to be the world's best networking company by meeting its customers' ever-increasing demand for reliable and secure connections throughout the world. Domestically, CenturyLink is the second largest provider of communications services to global enterprise customers. We provide a comprehensive suite of communications services to business, government, and wholesale customers in more than 350 metropolitan areas in the United States. We are also one of the largest Internet backbone providers. As a trusted partner, we help our customers manage increasing network and IT complexity and provide a robust set of managed network and cybersecurity solutions for organizations of various sizes. CenturyLink thus is a key

¹ National Telecommunications and Information Administration, International Internet Policy Priorities, Docket No. 180124068-8068-01, RIN 0660-XC041, 83 Fed. Reg. 26036 (June 5, 2018); 83 Fed. Reg. 27313 (June 12, 2018). Given their length, CenturyLink has included hot links to the sources cited in this submission so that they can be accessed electronically in their full form by both the staff of NTIA and other parties participating in this proceeding.

participant in both the domestic and global Internet ecosystem, helping enable digital innovations that increase prosperity, creativity, and civic engagement of people throughout the world.

CenturyLink is a member of the United States Council for International Business (“USCIB”), which is composed of more than 300 multinational companies, law firms, and business associations, reflecting a broad cross-section of the information and communications technology sector. We support USCIB’s comments in this proceeding. In this filing, CenturyLink highlights certain issues of concern featured in the NOI, including the free flow of information and jurisdiction, privacy and security, and emerging technologies and trends.

I. The Free Flow of Information and Jurisdiction

Growth in the Internet-based economy is unquestionably a fundamental component of GDP expansion in nations throughout the world, including in developing countries. Global e-commerce reached nearly \$28 trillion in 2016.² Cisco predicts that global IP traffic will triple between 2017 and 2021, with 3.5 networked devices per capita by 2021.³ This growth depends on the free flow of data and information, as NTIA recognizes in its NOI. Between 2002 and 2012, cross-border Internet traffic grew by 60% per year.⁴ A 2016 McKinsey report concluded that data flows increased global GDP by \$2.8 trillion in 2014.⁵ Such free flow is not only critical for the U.S. to maintain its leadership position in the global digital economy but also to help consumers and businesses around the globe realize the full potential of the Internet.

The NOI identifies several types of restrictions on the free flow of information, including censorship and barriers to the use of virtual private networks. Another concerning restriction is the increasing adoption of data localization mandates by foreign governments, requiring

² United States International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions* at 13 (USITC Publication 4716, August 2017), available at: <https://www.usitc.gov/publications/332/pub4716.pdf>.

³ Cisco, *Cisco Visual Networking Index: Forecast and Methodology, 2016-2021*, September 15, 2017, available at: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html#_Toc484813987.

⁴ Susan Lund, et al., McKinsey & Company, *The E15 Initiative: Strengthening the Global Trade and Investment System for Sustainable Development: How Digital Trade is Transforming Globalization* at 1 (January 2016), available at: <http://e15initiative.org/wp-content/uploads/2015/09/E15-Digital-Economy-McKinsey-FINAL.pdf>.

⁵ James Manyika et al., McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* at ii (2016), Executive Summary available at: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Executive-summary.ashx>.

companies to store or process data within the country and/or acquire individual or government consent for data transfer. For example, China passed a cybersecurity law in 2017 that requires a range of companies to store individual personal information and other “important” data within China.⁶

Such localization requirements ostensibly are intended to safeguard the personal data of the country’s citizens. Regardless of their actual purpose, these mandates directly inhibit global commerce and ongoing growth of the digital economy. For example, the European Centre for International Political Economy (“ECIPE”) previously estimated domestic GDP losses of 0.1% to 1.7% in jurisdictions that have adopted such policies, due to the increased cost of doing business in those areas.⁷ ECIPE further estimated losses in domestic investment from these policies of up to 4.2%.⁸

CenturyLink recognizes its responsibility as a global communications provider to secure and protect the personal data and information of its customers, regardless of their nationality, and has adopted best practices to do so. These best practices do not depend on data being stored in a particular jurisdiction and, in fact, can be hampered in some circumstances by jurisdictional restrictions that impede the aggregation of data to investigate cyber threats.⁹ CenturyLink therefore urges NTIA to work through multilateral organizations and other global discussions to minimize data localization requirements, including those that require use of local data centers, local content requirements, and procurement preferences for local companies.

II. Privacy and Security

Consumer confidence in online privacy and security is essential to global adoption and growth of the Internet. CenturyLink also agrees with NTIA’s perspective that cybersecurity risks are a threat to economic growth and innovation, as well as U.S. national security. CenturyLink therefore supports NTIA’s participation in global multi-stakeholder forums working to develop frameworks for privacy protection. Some variation in privacy regulation is inevitable, but these regulatory frameworks should be interoperable and avoid inhibiting global commerce.

For example, CenturyLink supports NTIA engagement in the Organization for Economic Co-operation and Development’s (“OECD’s”) upcoming review of its 2013 Privacy Guidelines

⁶ See He Huifeng, South China Morning Post, *Cybersecurity Law Causing “Mass Concerns” Among Foreign Firms in China* at 1 (Mar. 1, 2018), available at: <https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china>.

⁷ Matthias Bauer, European Centre for International Political Economy, *The Costs of Data Localisation: Friendly Fire on Economic Recovery* at 2 (2014), available at: http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf. The jurisdictions studied included Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam.

⁸ *Id.*

⁹ See USCIB Comments at 11.

during the 2019-2020 period. The original OECD Privacy Guidelines were the first internationally agreed upon set of privacy principles. They were updated in 2013 to reflect growth in the use and distribution of personal data. CenturyLink also encourages NTIA's engagement in the process that has begun between the European Commission and the Data Privacy Subgroup of the Asia-Pacific Economic Cooperation ("APEC") Electronic Commerce Steering Group to update the Referential mapping of the similarities between APEC's Cross-Border Privacy Rules and the European Union's General Data Protection Regulation.

CenturyLink believes that the recently revised National Institute of Standards and Technology ("NIST") Cybersecurity Framework provides a solid foundation for a voluntary security framework at the international level. A voluntary, rather than prescriptive, framework is essential to counter evolving threats. Avoiding a fractured regulatory regime also will allow companies such as CenturyLink to develop consistent, effective cybersecurity policies while minimizing compliance costs.

New potential cybersecurity vulnerabilities arise in a variety of contexts, including those introduced through global supply chains. While ongoing scrutiny of these supply chains is warranted, particularly for vendors or outsourced service providers, it is critical to avoid categorical prohibitions that may provide little, if any, improvement in cybersecurity while potentially imposing substantial compliance costs on network operators that previously relied on such suppliers in good faith. Such restrictions generally should not apply, for example, to equipment that lacks the capacity to harm the service provided, to route or redirect traffic, or allow visibility into the user data or packets it transmits. Network operators also should not be penalized for the practices of other domestic or international carriers from which they purchase backhaul, roaming, interconnection, or other services. Further, any restrictions and/or prohibitions on the use of specific vendors or service providers should not be contemplated until it is fully understood whether such measures would likely undermine the position of U.S. companies in the global markets or lead to counter-prohibitions against U.S. vendors. Instead, it is imperative that the United States lead the way in advancing risk management and mitigation practices to address new and existing cybersecurity vulnerabilities in a manner that recognizes the global environment we operate within and fosters an ongoing partnership between industry and government to identify discrete threats and address them. CenturyLink strongly recommends that NTIA coordinate its positions on potential cybersecurity vulnerabilities with other federal agencies and particularly the Department of Homeland Security.

III. Emerging Technologies and Trends

Led by U.S. industry, the digital economy continues to generate a spectrum of productivity enhancing innovations, including in artificial intelligence, machine-to-machine learning, and the Internet of Things. CenturyLink supports NTIA engagement in international forums on these emerging services, especially as a means of encouraging regulatory restraint. Regulation simply cannot keep pace with technological innovation, particularly for technologies in early stages of development. Governments should instead look to self-regulation and multi-stakeholder models, with resort to prescriptive regulation where these more flexible and nimble governance models have proven ineffective.

Ms. Fiona Alexander
July 17, 2018
Page 5

IV. Conclusion

CenturyLink appreciates NTIA's international engagement on the issues discussed above and is grateful for the opportunity to provide these comments on the NOI. We look forward to continuing our work with NTIA, other U.S. government agencies and interested businesses and civil society organizations through the international multi-stakeholder process to advance a growth-oriented agenda for the global Internet economy.

Very truly yours,

A handwritten signature in black ink, appearing to read "R. Edward Price". The signature is written in a cursive style with a large initial "R".

R. Edward Price