



July 16, 2018

Ms. Fiona Alexander
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC 20230

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

Dear Ms. Alexander:

The U.S. Council for International Business ([USCIB](#)) is pleased to respond to this request for public comments concerning NTIA's International Internet Policy Priorities for 2018. USCIB is a trade association composed of more than 300 multinational companies, law firms, and business associations, which includes a broad cross-section of the leading global companies in the information and communications technology (ICT) sector. USCIB members, which include parties to the non-contracted and contracted houses of ICANN, welcome this opportunity to offer a cross-community, cross-sectoral perspective on NTIA policy priorities for the Internet ecosystem.

USCIB members believe that digital technologies and the online environment enabled by them present unprecedented opportunity to raise productivity, foster creativity and innovation, generate economic growth, build trust, and enhance social prosperity. Key to realizing these social and economic benefits, however, are policies that ensure an open, safe, highly secure, stable, interoperable, seamless, and sustainable Internet that is based on the rule of law.

Such policies are most effectively developed when informed by stakeholder engagement through multistakeholder processes. The global Internet ecosystem benefits when government policymakers work in close cooperation with business and other stakeholders to develop and ensure that the legal, policy, and regulatory approaches adopted and implemented result in a holistic framework. Such a framework best enables sustainable business investment in infrastructure and innovation in legitimate/lawful products and services, includes technically feasible solutions, and offers appropriate privacy, security, and human rights protections, including privacy, intellectual property, and expression. At a time when the multistakeholder approach to Internet governance increasingly is challenged in certain multilateral forums, NTIA's solicitation of public comments of International Internet Policy Priorities is welcomed and very timely. We have organized our comments according to the four proposed categories:

I. The Free Flow of Information and Jurisdiction

- *Economic and Developmental Benefits* – USCIB embraces the view that the free flow of data and information is critical for economic development and growth. We urge NTIA to advocate in bilateral and international trade negotiations as well as in global forums such as the OECD, the United Nations, World Trade Organization (WTO), Association of Southeast

Asian Nations (ASEAN), the Asia Pacific Economic Cooperation forum (APEC) and others in support of policies that facilitate the adoption of new technologies and the global movement of data and information that support them. These policies will enable all citizens and companies to realize the full potential of the Internet as a platform for innovation and economic growth.

According to one study, the Internet and the data flows that support it have accounted for 15-20 percent GDP growth in many countries, including developing countries.¹ Other analysis reinforces this finding, highlighting the undisputed impact of data flows, within and across borders, on large-scale economic development as well as the improvement of the day-to-day management of companies of all sizes through business innovation, economic growth, and job creation.²

We note that the importance of the free flow of information was the *first* element of the [OECD's 2016 Cancun Ministerial Declaration](#) on the Digital Economy, which USCIB members shaped through their participation in Business at OECD (BIAC):

1. Support the free flow of information to catalyze innovation and creativity, support research and knowledge sharing, enhance trade and e-commerce, enable the development of new businesses and services, and increase people's welfare through policies, grounded in respect for human rights and the rule of law, that reinforce the Internet's openness, in particular its distributed and interconnected nature, while respecting applicable frameworks for privacy and data protection, and strengthening digital security ...

In recent years, the proliferation of government-mandated requirements to process or store data locally, require use or development of technology locally, and mandate use of local content or compliance with specific technical requirements have emerged as onerous barriers to cross-border flows of data and information. Some research has endeavored to quantify the negative economic impact of these policies. For example, the European Centre for International Political Economy (ECIPE) estimated GDP losses due to data localization policies may have a significant domestic impact in Brazil at -0.2 percent, China at -1.1 percent, the EU at -0.4 percent, India at -0.1 percent, Indonesia at -0.5 percent, Korea at -0.4 percent, and Vietnam at -1.7 percent. The research focused solely on the costs of doing business in those jurisdictions based on adoption of data localization policies.³ Studies also have estimated that data localization policies would reduce global trade by \$93 billion annually.⁴ The upshot is that data localization greatly increases the costs of doing business in that country – to the detriment of that country.

The preliminary draft report of the B20 Digital Economy and Industry Task Force (DEI Task Force) further highlights the negative *cross-sectoral* impact of data localization policies since many sectors of the economy rely on digitally supplied services and goods.

“Manufacturing, agriculture and other exports sectors are dependent on having access to a broad range of services at competitive prices – such as logistics, retail

¹ McAfee, Andrew and Erik Brynjolfsson (2012): “Big Data: The Management Revolution.”

² Brookings Institution (2014): “Supporting the Internet as a Platform for International Trade.”

³ ECIPE occasional paper No. 3/2014 (2014): The costs of data localization: friendly fire on economic recovery.

⁴ UNCTAD Information Economy Report 2015: “Unlocking the Potential of E-Commerce for Developing Countries,” March 2015.

distribution, finance or professional services – which in turn are heavily dependent on secure, cost-efficient and real-time access to data across borders. When data must be confined and stored within a country, it does not merely affect social networks and email services, but potentially any business that uses the Internet to produce, deliver, and receive payments for their work, or to pay their salaries and taxes. The idea that data should be stored only within one country falls apart as soon as a business representative or citizen crosses a border and finds that they no longer have continuous access to their data.”⁵

Business will comply with applicable privacy legislation and recognizes its responsibility to adopt recognized and applicable best practices to ensure that personal data and information is appropriately secured as technology and services evolve. Businesses endeavor to meet their customers’ expectations, so USCIB further acknowledges the importance of ensuring privacy and personal data protection. Countries that erect data localization barriers frequently cite privacy and security concerns as justification for them.

Business realizes that the benefits of technology innovation enabled by data flows will only be realized and embraced by consumers, businesses, and governments who trust the online environment and feel confident that the privacy of their personal data will be respected. This is best achieved through an appropriate balance such that the pursuit of privacy and security protections do not result in unnecessary barriers to data flows and the accompanying commercial, economic, and societal benefits.

We note that Article XIV of the General Agreement on Trade in Services (GATS) contains an exception for measures that may otherwise violate a GATS obligation provided they address a compelling public policy issue, including privacy and security. The GATS adds an important proviso that the measure in question must be proven to be “necessary” for the pursuit of a policy objective. This caveat is included to ensure that the pursuit of privacy and security policies do not result in policies that create arbitrary, discriminatory impediments to trade and data flows.

We urge NTIA to work closely with the Office of the U.S. Trade Representative (USTR) and the State Department to align interagency coordination and maximize the effectiveness of US Government advocacy in trade negotiations, policy work at multilateral organizations such as the OECD and APEC, and in other global discussions to support cross-border flows of data and information. Furthermore, we urge NTIA to remain committed to realizing a *trade principle*, with the underlying objective of allowing the flow, storage, and handling of all types of data across borders -- subject to a balanced and fair application of privacy and security laws consistent with Article XIV of the GATS.

- *Challenges to Freedom of Expression Online* – With the advent of the Internet and evolving digital transformation of the economy, USCIB members have sought opportunities to work with governments, regulators, non-governmental organizations, and others to meet the evolving challenges posed by new technologies and to carry out due diligence to help ensure that the Internet is used to foster an exchange of ideas. USCIB members are strongly committed to human rights. We will continue to advocate for both the governments’ duty to protect, and the corporate responsibility to respect human rights, in line with the UN Guiding Principles on Business and Human Rights.

⁵ Digital Economy and Industry 4.0 Task Force Policy Paper Draft, as of June 21, 2018.

Restrictions on freedom of expression, beyond those legitimately established to protect the rights of others, dampen the exchange of ideas, undermine public accountability, and reduce innovation and commercial opportunities. To promote freedom of expression and ensure that all human rights are respected online USCIB urges the following:

- Governments should address human rights issues with other governments directly;
- Governments should adopt the principle that offline laws and rules apply equally online and on the Internet;
- Governments should recognize the importance of the free flow of information in enabling the rights of expression;
- Freedom of expression online and the free flow of information should respect the rights of others and rule of law and should not be used as a rationale for abridging the rights of others, especially for commercial gains; and
- Policies should recognize that there are appropriate limitations to the right of free expression for the purpose of protecting the rights of others when implemented consistent with international treaties.

Concerning the final point, in particular, USCIB urges NTIA to leverage its participation in the International Telecommunication Union (ITU). Although the ITU does not have the mandate to serve as a “human rights forum,” we encourage NTIA to use the opportunity provided by ITU meetings to broaden its network of allies to oppose policies promoted by known human rights abusers. Ideally, this would be complemented by participation in as many relevant study groups as staff and resources allow to beat back proposals aimed at expanding ITU jurisdiction over Internet-related issues.

In our view, the reason some countries seek to promote an expansion of ITU jurisdiction over cybersecurity and Internet-related issues is often driven in part by their desire to control content distributed online and more readily surveil known and potential dissidents. The ITU Plenipotentiary, which will take place October 29-November 16, 2018 in Dubai, will offer even more opportunities to expand a “coalition of the willing” to oppose resolutions that ostensibly are aimed at addressing security and privacy concerns, but in fact are intended to pave the way for policies that restrict information flows and online expression.

The Internet Governance Forum (IGF), which will take place November 12-14, 2018 in Paris, will serve as another forum to advocate for the free flow of information and freedom of expression. Senior NTIA officials could address this topic as main session and workshop speakers. The IGF also offers opportunities for bilateral meetings with governments and civil society groups. The civil society groups could readily advise on perpetrators of online expression limitations, technologies used, and possible redress.

- *Jurisdictional Challenges on the Internet* – We agree that in the global borderless Internet, jurisdictional challenges are multiplying and complicating efforts to address freedom of expression and human rights concerns. Some USCIB members have been supporters of the [Internet & Jurisdiction Policy Network](#) (IJPN) which has produced extensive written analysis and hosted conferences exploring jurisdiction on the Internet. We encourage NTIA to continue to engage with the IJPN and help drive stakeholders to practical solutions.

II. Multistakeholder Approach to Internet Governance

- *Importance of Multistakeholder Approach* – To reiterate the main point of our introductory comments, USCIB believes that the multistakeholder approach to Internet governance continues to be the best method to support an environment for the Internet to grow and thrive and catalyze the development of policies that are timely, scalable, and innovation-enabling while ensuring that the online world is people-centered and inclusive.

The perspectives provided by business, civil society, the technical community, and government produce a flexible policy environment critical to empowering the rapidly evolving digital economy. Importantly, such stakeholder inclusion can lower the risk of unintended consequences⁶ and increase legitimacy and adoption of policies. Top-down government imposed policies and regulations often cannot keep pace with technological breakthroughs and can serve as a drag on development and innovation, and potentially infringe upon fundamental human rights. Self-regulation that provides transparency and accountability can often be a better solution to challenges in a rapidly changing marketplace. Having said that, we recognize there may be a need for legislation/regulation in certain well-defined areas, including where self-regulation has proven to be ineffective over time.

USCIB recommends multistakeholder processes at the national, regional, and international levels that are consistent with the following principles:

- Processes should be open, inclusive, transparent, and accountable;
 - Processes should enable all relevant stakeholders to participate, engage, and contribute to the discussions and decision-making, as appropriate to the forum and matter in question;
 - While recognizing that there is no single “best” multistakeholder model, participants should work to ensure a shared understanding among stakeholders of the issues and a desire to collaborate to address the issues.
 - Processes should involve local stakeholders (civil society, individuals, academia, local government and local business) in a meaningful way. In addition to raising awareness about cultural sensitivities, these stakeholders understand the issues that must be addressed at the grass- roots level and the opportunities that can be leveraged to achieve a positive outcome.
- *Accountability of Multistakeholder Approach* –The existing accountability structures within Internet governance organizations in which USCIB has been active over the years, e.g., ICANN and the IGF, are sufficient.

As will be discussed below, ICANN’s stakeholder community developed accountability structures to govern ICANN following NTIA’s transition of the IANA Stewardship functions. Having actively contributed comments throughout the two-plus-year development of the transition process, USCIB members remain committed to having the ICANN community hold ICANN’s management and Board of Directors accountable for policy actions and technical management of the domain name system (DNS).

⁶ For example, business can offer advice concerning possible negative economic, technical or commercial impacts of a proposed policy about which governments may not be aware in proposing the policy.

The IGF's program-related accountability structures are solid. This structure features observer access to deliberations of the Multistakeholder Advisory Group (MAG) and provides written transcripts of the proceedings that are available to the public. In addition, IGF workshop applicants are provided a "scorecard" to explain the subsequent rankings, which elaborate on the strengths and shortcomings of workshop proposals and the extent to which they met criteria requiring a diversity of speakers across stakeholder groups and regions. This ensures that issues and challenges in Internet governance are appropriately informed by various viewpoints and not dominated by one stakeholder group.

- *IANA Stewardship Transition and NTIA's ICANN priorities* – USCIB strongly disagrees that the IANA Stewardship Transition should be "unwound." USCIB members actively contributed comments throughout the two-plus-year development of the transition process. We issued a public statement endorsing the March 10, 2016 final package, expressing confidence that NTIA's criteria for the transition of the IANA stewardship role would be met and would ensure the continued stability, security and resiliency of the DNS as well as the fundamental openness of the Internet. Equally important in USCIB's view, the March 10 package included significant and concrete safeguards to enable active involvement by the community in processes designed to hold ICANN accountable as an independent entity.

We followed these statements with a positive acknowledgment of NTIA's June 9, 2016 announcement that the IANA Stewardship Transition proposal, indeed, met the criteria NTIA set forth in announcing its intention to transition the U.S. stewardship of the DNS technical functions to the global multistakeholder community. In the final analysis, the IANA Stewardship Transition was a monumental undertaking by ICANN's global community – most of whom contributed tirelessly as volunteers – and represented a noteworthy success of the multistakeholder approach to Internet governance.

The accountability mechanisms remain viable, but need to be respected by ICANN Org and the ICANN Board. NTIA plays a key role in ensuring that ICANN remains committed to fulfilling the obligations it made during the IANA stewardship transition. In line with its mandate to serve the global public interest and preserve the security and stability of the Internet, ICANN's actions need to effectively balance the diverse viewpoints and input from the global multistakeholder community, including that of governments, the business communities, and others, alongside the interests of the domain name industry.

While ICANN needs to improve, there is nothing to be gained by reversing the transition. Quite the contrary. Efforts to unwind the transition risk disrupting the security, stability and resiliency of the DNS system.

- *NTIA's Priorities within ICANN and the Governmental Advisory Committee (GAC)* – In general, it is very important that NTIA continue to reiterate strong support for the multistakeholder approach to Internet governance and uphold U.S. interests through its participation in the GAC and, where applicable, the GNSO policymaking process. In recent years, some governments have tried to weaken stakeholder participation in the ICANN policymaking process and governance of the Internet more broadly on grounds that this is best carried out by an intergovernmental body. It is critical that the U.S. Government be "present" as a GAC member and forcefully counter any such efforts in ICANN.

The U.S. Government must work to ensure that the DNS continues to be a safe, secure, and reliable platform for innovation and expression. Since the IANA transition, NTIA has expertly maintained a strong U.S. presence within ICANN on vitally important issues. The United States possesses the gravitas, influence, and technical understanding of DNS management to ensure that this central feature of ICANN's governance is not undermined. In particular, we commend NTIA for providing cogent recommendations regarding the treatment of geographic names in the DNS, and for being a leading voice on preserving access to (WHOIS) domain registration data for GDPR-allowed legitimate uses, such as consumer and intellectual property protection, cybersecurity, and law enforcement needs.

In terms of specific GAC priorities, USCIB urges NTIA to play a leading role to ensure that ICANN Org resolves disagreement with the recommendations raised in the GAC consensus advice from its [San Juan Communiqué](#) and [Panama Communiqué](#) regarding WHOIS and the EU General Data Protection Regulation (GDPR). The purpose would be to meet ICANN's stated goal of preserving access to registration data currently contained in the WHOIS framework to the greatest extent possible.

As ICANN itself highlighted in the statement accompanying the [Temporary Specification for gTLD Registration Data](#) (Temp Spec) issued on May 17, 2018, fragmentation of the WHOIS system would jeopardize the availability of registration data, which is essential to ensuring the security and stability of the Internet since access to this data enables easy identification of cybercriminal activity, intellectual property infringement, and other malicious and destabilizing online activity. We would add that WHOIS data is a tool for ensuring prompt, real-time action to mitigate cyber-attacks, many of which are supported by state actors.

Missing from the Temp Spec and only referenced in the Annex, however, is a process to develop both short-term and long-term mechanisms that provide a unified method for accreditation and access to registration data for GDPR-allowed legitimate uses. Short-term access to full WHOIS contact records for legitimate purposes is especially critical in view of the disruption caused by ICANN in adopting the Temporary Specification. We urge NTIA to lead GAC efforts to rectify this.

- *Barriers and Improvements to IGF* – Since its inception, the IGF has served as a pioneering example of cooperation among Internet governance stakeholders. Through its focus on the sharing of knowledge and ideas rather than on the development of prescriptive outcomes, the IGF has had the freedom to serve as an important laboratory for the discussion and dissemination of best practices and capacity-building initiatives that further the goals of the World Summit on the Information Society (WSIS) of expanded interconnectivity and inclusiveness. This invaluable feature must be preserved, while at the same time considering how the IGF may be improved.

USCIB believes a significant barrier to robust engagement at the IGF has been the cost to attend. This is due, in part, to the remote locations that historically have been selected to hold the conference. For more than a decade, the majority of IGF conferences have been held in parts of the world that are not easy to reach (e.g., Baku, Bali, Joao Pessoa, Nairobi) requiring expensive airfare and hotel accommodations. This, in turn, has limited the participation of potentially qualified and experienced IGF workshop speakers – from academia, for example -- because the workshop organizer typically is not able to cover transportation and housing costs. The high transportation costs of simply getting to the IGF have limited opportunities to involve both government and non-government participants

from developing countries. This has had the effect of undermining efforts to develop a more diverse base of participants that it is critical to informing bottom-up, self-governance in addressing Internet-related issues.

The Internet Society (ISOC) developed an Ambassadors Program to enable talented young ICT professionals to participate in the IGF. In addition, ISOC spearheaded the establishment of the Internet Governance Forum Support Association (IGFSA), which serves as a channel for additional funding to support and sustain not only the global IGF but also national and regional IGF conferences. The former only covers a relatively limited number of participants and the latter has not garnered sufficient funds to make it easier for non-traditional IGF participants to apply and secure financial support. In addition, not all organizations that participate in the IGF have the financial resources or fund-raising capabilities to underwrite similar efforts.

USCIB encourages NTIA to consider supporting policies that would help to resolve the financial barriers. Examples of such policies include:

- *Establishing an IGF Travel Fund* -- This fund could assist potential IGF attendees to apply for support based on the need of the attendee or organization.
- *Improve the IGF's own Financial Resources* -- The IGF needs to broaden the pool of funding resources to establish adequate long-term funding. This would provide the IGF Secretariat with sufficient resources to prioritize IGF topics of relevance to the community, ensure adequate documentation of policy discussions and best practice recommendations, and communicate its materials effectively. More stable and higher funding levels could also be used to not only establish a travel support fund, but also to develop much-needed website capabilities that would enable more effective archiving and retrieval of Internet governance-related materials. In addition, funds to expand website capabilities would provide more opportunities for remote participation by those who would like to participate but are unable to attend in person.
- *Advocate for Greater Transparency of U.N. rules concerning IGF Funding/IGF Site Selection* – The UN rules and processes related to IGF funding and the IGF Trust Fund account are complicated and opaque. Stakeholders and donors need greater clarity about how the Fund is used, how to make contributions to the Fund, and how the Fund is managed. Similarly, the procedures for the IGF meeting site selection process should be more open and transparent as it is often the need for sufficient funding that dictates where an IGF is held.
- *Discourage the Development of New Internet Governance Mechanisms or Models that Duplicate Existing Efforts Underway at the IGF* – Examples of duplicative efforts include the NetMundial Initiative and its World Economic Forum successor. There is a risk that establishing new mechanisms without a thorough and methodical assessment could drain resources – not to mention cause confusion among stakeholders – and result in reduced participation in the IGF. Rather, efforts to expand and strengthen the financial foundation of the IGF will enable the forum to expand existing mechanisms and address cutting-edge issues in Internet governance.

In terms of improvements to the IGF's structure and governance, we underscore the importance of solidifying the procedures and composition of the Multistakeholder Advisory Group (MAG). Although there are high-level criteria available concerning the UN's process for MAG appointments, each constituency group has its own unique process for making MAG recommendations. These procedures should be collected and shared with all

stakeholders. The UN's selection criteria should be clear, and the selection process transparent. In addition, issues of a MAG mandate and operational processes that reflect the multistakeholder nature of the MAG should be promulgated to better articulate responsibilities, expectations, and commitments for MAG participation.

Furthermore, we note a growing imbalance of views as reflected in the number and focus of workshop topics proposed by members of civil society. For all intents and purposes, the IGF in recent years has become overwhelmingly dominated by civil society and its priority agenda. Of the 300-plus workshop proposals submitted for the 2018 IGF, the MAG ultimately will select only 60. Of those 60 workshops, we remain concerned about a heavy slant toward topics and perspectives not necessarily shared by the other stakeholder groups. NTIA should use its position on the MAG to develop an approach to workshop and speaker selection that produces a fairer balance of stakeholder viewpoints.

Finally, we would encourage NTIA to continue to engage in the IGF and encourage its fellow colleagues from other regions to do the same. Having high-level officials and Ministers participating at the annual IGF meeting will help attract other stakeholders as well and keep the meeting relevant.

- *Role of Multilateral Organizations in Internet Governance* – In general, USCIB believes that it is critical for business to have a seat at the policymaking table to help ensure that policies are commercially feasible and foster growth, continued innovation, and creativity. Multilateral organizations, such as the ITU, the OECD, and the World Bank, in recent years have been actively exploring digital economy and related Internet governance issues.
 - OECD -- The OECD Committee on Digital Economy Policy (CDEP) recognizes stakeholder participation from government members, business, the technical community, and civil society. USCIB is the U.S. business participant in Business at OECD (BIAC), the OECD-recognized business stakeholder group. BIAC regularly contributes comments to CDEP documents and is recognized by the CDEP Chair to make interventions during meetings. Because of this inclusiveness, the OECD has produced important Internet-related initiatives that continue to enjoy broad stakeholder and government support. Specifically, the 2011 [Internet Policy Principles](#) (IPP) have served as enduring guidance to nations and organizations grappling with challenges in Internet governance. Most notably, the IPPs served as the basis for compromise language on key elements of the [2015 NetMundial framework](#), such as the provision on Internet Intermediary Liability.

The OECD's [2016 Cancun Ministerial](#) considered the opportunities and challenges presented by the digital transformation of the economy and society that culminated in a declaration calling on the OECD to provide its government members “with strong evidence and innovative analysis needed to develop sound policies to achieve our objectives and contribute to a flourishing digital economy.” The OECD's follow-on [Going Digital Project](#) aims to give policymakers the “tools they need to help their economies and societies prosper in this increasingly digital and data-driven world.” USCIB/BIAC actively has provided input to both. More recently, USCIB/BIAC feedback directly influenced improvements to the structure and substance of the Going Digital Project's Integrated Policy Framework.

- ITU -- The ITU plays a very important role in allocating global radio spectrum and satellite orbits, developing the technical standards that ensure networks and

technologies seamlessly interconnect, and improving access to ICTs to underserved communities worldwide.

Some Member states have endeavored to expand the ITU's role in international Internet governance, however. This is highly problematic for business and detrimental to key sectors of the US economy. In a [public statement](#) issued by USCIB prior to the World Telecommunication Standardization Assembly (WTSA), we urged the U.S. Government to advocate against WTSA Resolutions that would expand the scope of Study Group work and effectively open the door to inappropriate and counterproductive ITU work that is well beyond its current remit, including matters relating to Internet governance and policy.

USCIB followed this up during the [August 2017 Open Consultation on Public Policy Considerations for OTTs](#), arguing against efforts to expand the ITU's jurisdiction and work programs to include Internet-related issues, such as online services and applications. We reiterated that expanding the ITU's work program beyond its current remit would compromise the Union's ability to meet its current goals. Yet, in the months leading up to the ITU Plenipotentiary (PP-18), October 29-November 16, 2018, in Dubai, business continues to see proposals from some countries and regions that aim at expanding ITU work into Internet-related issues.

As we noted in both sets of comments and highlight above, USCIB values and respects the ITU's primarily technical mission; its role in allocating spectrum, developing technical standards that ensure the interoperability of international telecommunication networks and promoting human capacity building in developing countries. We also recognize the importance of the ITU as a convener of global discussions on connectivity and policy matters in some form.

As we also emphasized earlier in these comments, however, Internet-related and digital economy issues are most effectively addressed in multistakeholder forums, where policy is holistically and expertly informed by consultations among business, civil society, the technical community, and government. Multilateral organizations like the ITU certainly are a stakeholder in Internet governance-related discussions – and the ITU, in fact, has contributed speakers to the IGF and co-organized IGF workshops. USCIB asks the US government, especially NTIA and the State Department, to remain vigilant in ensuring as much as possible that the ITU not stray outside of its traditional remit.

III. Privacy and Security

- *Cybersecurity Responses and Commercial Implications* -- Virtually all companies – digital content providers, software manufactures, ISPs, and digital platform providers as well as retailers, financial services and insurance providers, manufacturers, and delivery service providers, to name just a few – operate in the digital ecosystem and must contend with the evolving set of security challenges. The same holds for consumers and organizations who utilize online services to conduct business, purchase products, and engage with various communities.

As we discuss above, the proliferation of data localization requirements often is rationalized by the government as necessary to keep data and systems secure. Such policies are a

disproportionate response to security threats. In reality, they have the opposite effect of making the data storage more vulnerable to outside attacks.

The preliminary draft of the B20 DEI Task Force report observes that big data and machine learning have the potential to drive improvements in our understanding of cyber-threats as well as innovative defensive technologies and strategies. Importantly, the draft notes that when data are confined to a local environment, they cannot be aggregated and used to analyze the behavior or tools of malicious actors. As a result, “organizations that operate across borders may not be able to take advantage of scale to improve the security of their products and services, and groups of organizations, such as within a sector, will be limited in leveraging cross-border information sharing and in pursuing coordination on defense,” according to the B20 draft.⁷

The preliminary DEI Task Force paper also makes several recommendations on improving cybersecurity that focus on policy actions to help promote risk-based approaches and build resiliency in systems. Section 7.1 of the draft, for example, notes the need for government and industry partnership to align on cybersecurity approaches and cyber-risk frameworks. Avoiding a fractured regulatory regime and utilizing international standards that are consistent across borders will help global entities develop a forward-looking and meaningful view of the threat landscape, which will ultimately strengthen ICT systems (and trust in systems), and will reduce compliance burdens, the report states.⁸

Business acknowledges that data localization policies often are driven by a lack of trust in the online environment. USCIB members further recognize that they have a corporate social responsibility as well as commercial interests in building trust among consumers, governments, and other stakeholders. USCIB members therefore advocate that security risks are most effectively mitigated by a combination of technology innovation (security-by-design, use of big data), voluntary, risk-based cybersecurity frameworks (e.g., the NIST and OECD models), and best practices -- not by data localization requirements.

We urge NTIA to coordinate closely with other agencies focused on commercial and trade issues to hold countries that impose trade/data flows barriers on grounds of security accountable to their international trade commitments. The negative security and economic impacts of such requirements should be amplified.

- *Addressing Digital Privacy in International Venues* – As we note above, USCIB members recognize and embrace their responsibility to adopt recognized and applicable best practices to ensure that personal data and information is appropriately secured and protected. But we reiterate that there must be an appropriate balance so that privacy frameworks promote consumer/user trust in data-driven technologies while at the same time enable companies and organizations to use and transfer data in innovative ways that benefit society.

USCIB believes that the OECD’s 2013 Privacy Guidelines⁹ serve as a solid foundation for a national privacy and data protection framework through its inclusion of the principle of

⁷ Draft B20 Digital Economy and Industry 4.0 Task Force Policy Report, *op. cit.*

⁸ *Idem.*

⁹ Organization for Economic Cooperation and Development (OECD), *OECD Privacy Guidelines* (2013), <http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>

proportionality, among other measures appropriate for privacy in a digital age. Under the aegis of BIAC, USCIB actively contributed input that helped to shape the 2013 guidelines and will do the same when the OECD undertakes a review of this framework during the 2019-2020 period.

The OECD is an appropriate forum to consider and develop digital privacy frameworks because it recognizes and gives weight to the input of non-governmental stakeholders. Given the rapid pace of technological change, it is critical for business and the technical community to advise OECD member governments whether elements of a privacy framework are technically conceivable; civil society, in turn, will advise about whether the framework offers adequate personal privacy protections.

Perhaps most important, the OECD's evidence-based approach to policy development means that recommendations are based on economic analysis and metrics rather than on political prescriptions. This characteristic of the OECD's work has earned it respect from many non-member countries who likely will use the OECD framework as a model for their national approach. It comes as no surprise, therefore, that the B20 DEI Task Force likely will recommend that that OECD's Privacy Guidelines be used as a reference to develop greater interoperability in global privacy regimes. "Only a mutual recognition of privacy standards will enable the cross-border flow of data requires for an inclusive digital economy," the draft states.¹⁰

USCIB urges NTIA and the U.S. Government more broadly to participate in the OECD's review of the 2013 Privacy Guidelines during the 2019-2020 period and welcomes the opportunity to engage with relevant NTIA staff throughout this process.

For many of the same reasons, USCIB also encourages NTIA to participate in the Data Privacy Subgroup (DPS) of APEC's Electronic Commerce Steering Group (ECSG). Using the OECD's Privacy Guidelines as a basis, the DPS developed the [APEC Privacy Framework](#) and [Cross-Border Privacy Rules](#) (CBPR) system with input and assistance from business and civil society. The CBPR system requires participating companies to implement data privacy policies consistent with the APEC Privacy Framework, which must be assessed as compliant by an Accountability Agent (the Federal Trade Commission for U.S. companies) and enforceable by law. The most promising feature of the CBPR is its potential to emerge as a model for regulatory interoperability in the Asia Pacific region and elsewhere.

The European Commission evidently recognized this potential by agreeing to work with members of APEC's DPS to develop a Referential that mapped the similarities of the CBPR to the EU Binding Corporate Rules. The Commission and DPS members currently are scoping a project aimed at mapping the CBPR to the EU GDPR. It is important that NTIA coordinate within the interagency process to make sure that NTIA and other U.S. Government staff with privacy expertise participate in this initiative. USCIB, which contributed to the DPS's development of the CBPR, would welcome the opportunity to engage further with NTIA about this work.

¹⁰ Draft B20 Digital Economy and Industry 4.0 Task Force Policy Report, *op. cit.*

IV. Emerging Technologies and Trends

- *Importance of Artificial Intelligence* -- USCIB members regard AI technologies as computational intelligence that can help subject matter experts to make advances in every sector, enabling innovation and highly beneficial applications in healthcare, agriculture, education, manufacturing, and transportation, among other areas. Because technologies related to Artificial Intelligence (AI), virtual/augmented reality and others, in fact, are still “emerging” in their technical and commercial development, it may be inappropriate for any international venue to develop public policies or regulations to govern them. Such premature activity by the world’s governments could have unforeseen and unintended consequences that would stunt the growth of these emerging technologies and retard the benefits consumers could enjoy from their continued development.

For AI to be adopted and deployed on a global scale, it is essential that all stakeholders work together to shape the development of AI to foster trust and broad adoption, including educating people about its potential for societal good and addressing worries about job dislocation and the need for reskilling so workers can stay ahead of the technological curve and seize the benefits of AI transformation. Industry groups devoted to emerging technologies, such as the Partnership for AI, have formulated best practices on emerging technologies and advanced the public’s understanding of them. We also recognize that AI might pose other challenges as well.

It is important to keep foremost in mind the fact that broadband connectivity is a necessary prerequisite for using most emerging technologies. Thus, with 3.5 billion people still unconnected to the Internet, we urge you to consider that the world will be better served by international venues recommitting to expanding global connectivity.

- *International Venues for Discussions about Emerging Technologies – Artificial Intelligence* (AI) technologies, machine learning, the Internet of Things, and other emerging technologies have become hot topics in industry and intergovernmental conferences. AI technologies, in particular, were the focus of a conference, “AI: Intelligent Machines, Smart Policies,” jointly organized by the OECD and the Government of Japan in October 2017, and will be the centerpiece of an OECD study that will culminate in a Council Recommendation in 2019. In the Fall of 2018, the G7 Innovation Ministers also will have a Multistakeholder Forum on Artificial Intelligence. We encourage NTIA to become involved in this.

The ITU, in partnership with XPRIZE Foundation, the Association for Computing Machinery (ACM) and more than 30 other UN agencies and bodies, organized the “AI for Good Global Summits” in 2017 and 2018. The program considered how AI technologies can contribute to realizing the UN Sustainable Development Goals. However, the summits have been driven by the ITU Secretariat rather than by the membership itself, and they appear geared to positioning the ITU as a global leader of AI-related discussions. This aspiration is not shared by many in the business community as evidenced by the decision of several high-profile USCIB member companies to decline the ITU’s invitation to participate. In addition, the ITU Telecommunication Standard Sector’s Study Group 13 has taken on “Machine Learning for Future Networks.”

We note that the governments of China, Japan, the United Arab Emirates, and the United Kingdom have made high-profile announcements about plans to prioritize development of AI technologies.

AI-related discussions in various international forums have proposed that the UN needs a structured approach to AI and potentially a review of current UN frameworks in this context. We note the possibility of an AI-related resolution being considered at the ITU Plenipotentiary (PP-18) later this year.

USCIB does not support the development of AI policy recommendations or AI ethics principles in the UN General Assembly or any of its specialized agencies, including the ITU. The ITU should seek to focus its AI work on its core mandate, while also avoiding inefficient and costly duplication within existing and ongoing work on AI in the following forums:

- The OECD and Development AI Initiative, including the outcome of its conference, “AI: Intelligence Machines, Smart Policies” and its expert working group;
- The Institute of Electrical and Electronics Engineers (IEEE);
- The International Organization for Standardization;
- The Partnership on AI and other UN agencies including the United Nations Economic and Social Commission for Asia and the Pacific (UN-ESCAP), the United Nations Interregional Crime and Justice Research Institute (UNICRI) Centre for Artificial Intelligence and Robotics, and the United Nations Organization for Education, Science and Culture; and
- Numerous other industry forums, think tanks, institutes and academic conferences.

To the extent that the ITU explores AI within its remit, it should do so through multistakeholder consultations and dialogues, including considerations about how the ITU can help to share existing information and work on AI technologies with Member States, development and use of AI in the telecommunications/ICT infrastructure, how AI realizes the Sustainable Development Goals, and how the ITU can coordinate on an ongoing basis with respective organizations and UN agencies on AI technologies development.

We encourage NTIA to ensure that the G7 Multistakeholder Forum on AI, the G20 Summits, and the PP-18 endorse outcomes that enable growth and innovations of these technologies. This can be done by proactively promoting the development of AI through coordination and securing international investment in research and education, while also adopting frameworks that hinge on investing in human capital skills, and worker flexibility.

- *Policy Recommendations and Best Practices* -- USCIB emphasizes the following points made by BIAC at the OECD’s AI conference in October 2017:
 - The importance of ongoing multistakeholder dialogue between business, government, civil society, and the technical communities on how AI can be shaped to maximize its potential and mitigate its risks, including adoption of practical guiding principles to encourage development of human-centered AI and development of healthy ecosystems, including essential infrastructures to support application of AI technologies;
 - Stimulate the development and deployment of AI across all sectors and business of all sizes, including application of AI to address public and societal challenges, such as empowering underserved communities and those with disabilities, and adoption of AI in the public sector;
 - Develop privacy laws with a view toward enabling the benefits of AI while preserving privacy;

- Invest in skills development training initiatives for people at all stages of the job continuum;
- Encourage sharing and promulgating of best practices in development and deployment of human-centred AI, through industry-led organisations such as PAI;
- Fund short- and long-term multi-disciplinary research and development of human-centered AI technologies and how AI can be used to provide insights into its potential socio-economic impact.
- Develop shared public data sets and environments for AI training and testing, to enable broader experimentation with AI and comparisons of alternative solutions to address ethical concerns.

Importance of Evidence-Based Analysis -- We underscore that business is leading the development and innovation of AI systems and their deployment in all sectors, actively working with governments, academics, and civil society globally across many organizations. These efforts are aimed at helping to shape the development of AI in a way that can foster trust and broad adoption. It is critical that the issues raised by this emerging technology are informed by evidence-based analysis and perspectives of a range of business and other stakeholders.

As mentioned, the OECD currently is in the midst of a comprehensive study, “Artificial Intelligence in Society.” This project will provide evidence-based research and insights – informed by stakeholder inputs – that would serve as a sound foundation for developing thoughtful and balanced approaches to questions raised by AI technologies and how stakeholders can collaborate to shape their development.

In contrast, UN organizations will serve as platforms for some Members States to advocate how these promising technologies should be applied and regulated, in a setting that allows limited, if any, advice from knowledgeable stakeholders.

Industry and government must work together to develop medium- and long-term solutions to empower all people and sectors to participate freely, feel safe, and take advantage of the benefits of technological innovations like AI.

V. Conclusion

USCIB firmly believes that digital technologies and the Internet ecosystem hold great promise for the global economy and for society. We are grateful to NTIA for this request for public comment to provide the perspective of businesses who are innovators both of digital technology as well as use of the Internet platform. We reiterate that the keys to realizing economic and social benefits in today’s digital economy are policies that are informed by *all* stakeholders and are aimed at ensuring an open, safe, secure, stable and sustainable Internet based on the rule of law. Stakeholder guidance and evidence-based analysis is especially critical to ensuring that emerging technologies, such as AI, can be shaped to maximize its potential and mitigate possible risks.

We urge NTIA and the US Government more broadly to resist efforts by some governments to burden companies that have thrived in the digital ecosystem – and in so doing, created new jobs and improved the quality of life for many – with innovation-hampering regulations. The

government and private sector can realize a better future for the digital economy by working together.

Sincerely yours,

A handwritten signature in cursive script that reads "Barbara P. Wanner". The signature is written in black ink and is positioned below the "Sincerely yours," text.

Barbara P. Wanner
Vice President, ICT Policy

Copies to: Peter M. Robinson, President and CEO
Rob Mulligan, Senior Vice President, Policy and Government Affairs