Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, D.C. 20554

Notice of inquiry	)	
	)	
International Internet Policy Priorities	)	Docket No. 1810124068-8068-01
	)	RIN 0660-XC041

COMMENTS OF MICROSOFT CORPORATION

Introduction

Microsoft Corporation (Microsoft) appreciates the opportunity to provide comments to the Notice of Inquiry (NOI) issued by the National Telecommunications and Information Administration (NTIA), United States (U.S.) Department of Commerce, on International Internet Policy Priorities dated June 5, 2018. We would like to express our full support of NTIA's recognition of the vital importance of encouraging "*growth and innovation for the internet and internet-enabled economy"* and the need for international engagements on these issues. In this response, as there is no longer a clear distinction between the *internet-enabled economy* and the broader economy, and many of the policy issues being considered actually concern the *digital transformation* of the entire internet/digital ecosystem, we will also use this term and consider these issues in answering the questions posed by NTIA.

Experience has shown that where government and private sector resources are united in a common effort, the U.S. goals of realizing the full potential of the digital transformation and preserving U.S. competitiveness can be met. This NOI is a vital link between the government and the multistakeholder community. In this response, we have raised issues that are important to Microsoft due to their impact on our global commercial operations. We hope that they provide compelling evidence of the need for international engagements, and sufficient guidance for NTIA where it has authority. Where it does not, we urge NTIA to help advocate, on our behalf, that the Department of Commerce, other relevant agencies, and more broadly the U.S. government, prioritize these issues in their respective international engagements.

- **Microsoft's Business Strategy on Intelligent Cloud and Intelligent Edge**

With a mission to "*empower every person and every organization on the planet to achieve more*," Microsoft strives to create local opportunities, growth and impact in communities and countries around the world through digital transformation. Our tools and platform services are designed to empower human ingenuity to radically transform every sector from agriculture to manufacturing, enable new startups and innovative services, improve educational outcomes, and address major societal challenges. Our strategy of intelligent cloud and intelligent edge is foundational to achieving this vision and delivering services that are richer, contextual, and seamless across devices. Today, Microsoft's global Azure infrastructure spans 54 global regions – more than any other cloud provider – enabling services in 140 countries. The scale of the infrastructure brings applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for our customers.

At Microsoft, we are fundamentally optimistic about the potential of the cloud and how it can be used to drive societal and economic benefits. Recognizing that a lack of understanding about these technologies can cause concerns, in 2016 we launched "A Cloud for Global Good" – a set of policy considerations for how governments, industry, academics and civil society can work together to create a cloud that is trusted, responsible and inclusive. Policy issues addressed encompassed all the broad categories in this NOI – i.e., free flow of information and jurisdiction; privacy and security; emerging technologies such as artificial intelligence (AI); and the need to work across industry, with governments and other stakeholders, to find the right balance that can make technology work in the modern world, using mechanisms that include laws, regulations, standards, industry codes, best practices and certifications. We categorized these issues according to their contributions to making the cloud more trusted, responsible and/or inclusive. These recommendations were updated in Jan 2018 with learnings and new ideas gained from our engagements with leaders from governments, businesses, academia, and civil society around the world.

Microsoft's intelligent cloud and intelligent edge strategy rely on an internet that is interoperable, open, globally accessible to as many people as possible, and that remains safe, secured, and resilient as it continues to expand. Preserving such an internet is critical to its continued role as an innovation platform and an enabler of sustainable and inclusive economic development globally. The internet's openness is crucial to its continued growth and contributions to GDP in the US and worldwide. Over the decade to 2014, increased global flows of goods, foreign investment, and data increased world GDP by at least 10%, totaling $7.8 trillion in 2014 alone; of this amount, $2.8 trillion was due to data flows – larger than the share due to flows of goods.[1] The internet is the backbone of the global digital economy – a general-purpose technology that is the foundation of the ongoing digital transformation for organizations of all sizes, in every sector, in every country. Our cloud services and the quality of service that we can deliver to our customers (e.g., availability, reliability, security) rely on the smooth functioning of the internet infrastructure, and the minimization of geographically conflicting regulations affecting internet traffic (e.g., cross-border data flows, interoperable privacy frameworks).

- **Microsoft's International Engagements on Internet Policy**

For more than two decades, Microsoft has been an active participant in dialogues on policy issues related to internet governance globally, including at the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU), the Internet Governance Forum (IGF), the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), etc., advocating the need for multistakeholder approaches where government, business, civil society, the technical community, and other stakeholders, take part in public policy development. In countless engagements around the world, we partner with local business, governments, civil society, and others in projects worldwide to bridge the digital divides. We work on the supply side, to ensure provision of affordable and universal access to broadband services and the internet; as well as on the demand side, to build capacity for local communities to adopt, produce and consume localized content and services safely and inclusively, and to empower all people and organizations to access, participate and be fully-included in social, economic and political activities.

As technologies, including the internet, are perceived as exacerbating global inequalities and societal instability, governments around the world continue to pursue their policy objectives and as a result are

[1] McKinsey Global Institute, "Digital Globalization: The New Era of Global Flows," March 2016.

increasingly seeking to regulate U.S. business and innovations. Governments are also increasingly leveraging multilateral organizations and international forums to promote their policy agendas and to condition the policy environment to be more favorable to their strategies. More than ever, they are coordinating their engagements across multiple forums, i.e., raising policy issues in forums where it may be easier to have their agendas adopted, and then leveraging the outcomes elsewhere; the overall trend is towards greater government intervention and regulation.

- **Need for International Engagements from NTIA and U.S. Government**

For these reasons, others cited in the NOI, and as economies become increasingly interconnected, it is essential that NTIA and, more broadly, the U.S. government continue their strong and proactive engagements in international organizations to help support U.S. business and enable continued growth and competitiveness in this increasingly challenging environment. Increasing international co-operation and more effective forms of multilateral collaborations are necessary to restore the trust needed to achieve the full potential of the digital transformation. The U.S., with a policy environment that promotes market-based innovation, inclusive economic growth, and a preference towards ex-post regulation and enforcement, has led the world in deployment of digital technologies and experienced first-hand their impact on national GDP. This is contrary to some of the examples cited in the NOI, where governments seem to prefer siloed and ex-ante regulatory and policy approaches.

Differences between countries, coalitions of countries, and regions as to visions of the internet and the digital transformation are leading to internet fragmentation. As such, this NOI is very timely in bringing forward a discussion about the fundamental principles that should guide the global digital transformation. We suggest that holistic, enabling policy and regulatory frameworks that ensure consistent approaches across sectors and policy silos, that are integrated across government and across society and aimed at achieving sustained investment, inclusive economic growth, and societal well-being are necessary to realize the potential of the digital economy. The four focus areas of the NOI involve an interdependent economic, socio-cultural, technical, and governance system. Such frameworks should also consider the needs of the different stakeholder communities, including business, technical, civil society, and governments. These factors need to be balanced, and the analysis and policy recommendations must be grounded in evidence to realize the potential of digital transformation in a trustworthy and inclusive manner.

With significant experience in enabling economic growth from advancement of digital technologies, the U.S. government is one of few governments that can provide evidence-based leadership in international policy making on the digital transformation. To do so will require sufficient resourcing across a number of different agencies whose expertise are needed to address the issues raised in this response to the NOI, including NTIA and the Department of Commerce more broadly, the Department of State, the Federal Communications Commission, the Federal Trade Commission, the United States Trade Representative (USTR), and other essential and relevant agencies in the defense and technology communities. The need for sufficient resources is clearly seen when facing the considerable challenges that arise from having to take part in multiple international organizations, regional groups, and economic coalitions, as these forums evolve to consider the same set of issues related to the digital transformation. The upcoming ITU Plenipotentiary conference in Dubai this October is but a single example of the policy challenges that will arise.

In addition, consistency across agencies in recognition of the need to engage in international organizations and the ability to establish consensus positions through the inter-agency process are essential to establishing a strong U.S. presence in these international meetings, many of which business can participate in only by being a part of the U.S. delegation (e.g., the ITU and the UN).

Appropriate and strong U.S. representation at international meetings is also essential in light of investments from other governments in standards and policy-making international organizations, and their engagement through leadership and strategic positions within these organizations. As such, it is more important than ever to have pro-active U.S. government engagement and leadership on the global stage to drive a favorable and enabling policy and regulatory framework under which U.S. businesses can operate and thrive.

Executive Summary of Microsoft's Policy Priorities

Within the context of the need for holistic, enabling policy and regulatory frameworks that are focused on sustained investment, inclusive economic growth, and societal well-being, we raise the issues below for NTIA's consideration in prioritizing its international engagements. These issues are discussed in greater detail in the remainder of our comments.

1. <u>Free Flow of Information and Jurisdiction:</u>
   - *Cross-border data flow* – As economies and global value chains are increasingly interconnected, the ability to transfer digital information across borders is essential to economic growth, especially for businesses that are increasingly relying on a global network of cloud services. NTIA can help to advocate that a balance needs to be struck between encouraging e-commerce by facilitating such flows and preserving privacy, protecting individual and public safety, promoting national security, and respecting national sovereignty. Any rules must also consider the WTO moratorium on e-commerce duties and nondiscriminatory treatment for digital products and services, provide maximum flexibility, and create the least risk of conflicting national rules.
   - *Freedom of expression online* – When governments requests the removal of user content from cloud services, there should be clear laws and regulations that protect public safety, freedom of expression, and human rights – complementary values that reinforce each other, and are critical to the digital economy. NTIA should advocate that such laws must be transparent, and governments must adhere to the rule of law, and clearly define what constitutes illegal content and the types of services that must remove it. National sovereignty needs to be respected, and interference with technology companies' terms of use should be avoided.
   - *Cross-border domain takedown requests* – The number of requests to suspend cross-border domain names that are associated with illegal content or activities has been increasing. The lack of recognized international legal frameworks has exacerbated the challenge of addressing these issues. NTIA should remain vigilant to prevent attempts to leverage concerns about these very real cyber threats to impose inappropriate limits to freedom of expression through domain name suspension.

2. <u>Multistakeholder Approach to Internet Governance:</u>
   - *Importance of multistakeholder approach* – Multistakeholder approaches have driven the growth of the internet and enabled tremendous socio-economic progress. Such approaches are optimal in the development of policy frameworks where innovation in technology, business models, and markets is evolving quickly. Through open dialogues, stakeholders can identify and prioritize potential socio-economic and regulatory challenges and share responsibility on how to best mitigate these challenges by leveraging their respective unique expertise. NTIA should also advocate for balanced policy frameworks that consider a combination of self-regulations, voluntary- and market-driven technology standards, sharing of best practices, application of existing regulations, and where appropriate, updated policy and regulatory frameworks.

- *ICANN priorities* –
    - *IANA transition*: Microsoft welcomed the transfer of the stewardship over the IANA functions from NTIA to the global multistakeholder community as a significant and necessary development and sees no reason to "unwind" the IANA transition; indeed, such action would undermine the essence of the multistakeholder approach to internet governance and should therefore be avoided. ICANN needs to continue to be held accountable to the multistakeholder model, and we are confident that the conclusion to the Accountability CCWG's work will help ensure this happens.
    - *WHOIS compliance with the General Data Protection Regulation (GDPR):* Microsoft sees no conflict between GDPR compliance and the use of WHOIS data for legitimate and important purposes such as cybersecurity. We urge NTIA to continue to engage with ICANN to contribute to efforts to define permanent, practical, efficient and predictable solutions to bring WHOIS into compliance with GDPR, resulting in a mandatory, uniform access and accreditation solution as soon as possible.
- *Improvements to the IGF:* While acknowledging noticeable improvements as well as ongoing efforts to further enhance the IGF, we suggest that NTIA consider the following as areas that can further strengthen the IGF's role as the leading platform for multistakeholder dialogue on issues of importance to internet governance: (i) draw on existing strengths and outputs to increase the impact of the IGF; (ii) develop and implement a multi-year plan towards 2025; (iii) stabilize funding of the IGF; and (iv) address the declining engagement of governments and the private sector.

3. <u>Privacy and Security:</u>
    - *Cybersecurity:* Governments and international organizations should be encouraged to leverage industry-led cybersecurity risk management practices that are proven across sectors and around the world, including ISO/IEC technical reports that built on the widely-used NIST Cybersecurity Framework and the Microsoft Cybersecurity Tech Accord. In addition, NTIA should call attention to the economic impact of cyber-attacks and support efforts to work towards greater nation-state restrain in cyber-attacks.
    - *Privacy considerations and interoperability of frameworks:* A strong legal framework for data protection provides an essential foundation for data-driven innovation and entrepreneurship to flourish. Such foundation should integrate core principles to instill the level of trust needed to propel international trade, sustain economic growth and create new opportunities for everyone inclusively. We suggest key core principles for NTIA to consider in its work on privacy principles, in its participation in the OECD review of the Privacy Principles as well as other international forums.

4. <u>Emerging Technologies and Trends:</u>
    - *International venues for policy development on emerging technologies and trends:* No single multilateral organization has the competency or mandate to address all aspects of policy development for issues related to the internet or digital transformation. There needs to be an ecosystem of organizations with a variety of expertise, experience, and activities, working in a coordinated manner, leveraging each other's unique historical mandate and expertise. We urge NTIA to work with the Department of State and other appropriate agencies to ensure that U.S. business interests are strongly represented in these forums, and to shape the work in these organizations so that they are coordinated, not duplicative, in ways that are consistent with their mandates, core competencies and experience. Business input is essential to the development of policy and development of holistic policy and regulatory frameworks for inclusive and sustainable growth.
    - *Artificial intelligence:* For AI to be adopted and deployed on a global scale, its development needs to be shaped to foster trust and broad adoption. Based on the OECD's past work, its focus on the

economic context, and its evidence-based approach, Microsoft strongly endorses its initiative on development of human-centric AI policy and its efforts to develop principles that will enable trustworthy development and deployment of AI systems around the world. We urge NTIA to similarly endorse and firmly support this effort, including establishing the inter-agency consensus necessary to take leadership roles in shaping these activities. With governments around the world expressing increasing interest in AI, and especially in establishing regulatory and ethical frameworks, NTIA, and more broadly the U.S. Government need to actively engage in shaping the development of AI policy frameworks to preserve U.S. leadership and competitiveness. As AI is still at a nascent stage of development, open dialogues between government, business, civil society and academic researchers are essential to shaping the continued development of the technology and realizing its potential benefits. Policy discussions should aim to promote broad development and deployment of AI across different sectors and continued AI innovation, encouraging outcomes that are aligned with the vision of human-centered AI.

- *Online content, applications and services:* Online content, applications, and services should be embraced as part of a holistic framework for enabling investment and inclusive growth. We urge NTIA to continue its support of the critical role that online content, applications, and services play in the entirety of the internet economy and the benefits they produce. NTIA should continue to advocate against reflexively extending legacy regulation to the world of online content, applications, and services, and for eliminating barriers that can adversely impact the evolution of the internet ecosystem.

1 The Free Flow of Information and Jurisdiction

1.1 Economic Impact of Cross-Border Data Flow

As economies and global value chains are increasingly interconnected, the ability to transfer digital information across borders is essential to economic growth and opportunity. It is estimated that the global economic impact of the international flow of data may reach up to 11 trillion U.S. dollars by 2025 (from an estimate of 2.8 trillion USD in 2014 as cited from McKinsey above).[2] Studies have found that data-fueled technologies have the potential to drive a sharp increase in innovation, productivity gains and economic growth. Access to cloud-based technologies is especially important for small and medium enterprises, because it can enable them to compete against larger businesses and reach customers around the world in ways that were not previously possible. However, as noted in the NOI, governments are increasingly restricting cross-border data flows, with requirements on local storage, local processing, local access, or conditional restrictions on data flows, where data transfer abroad is forbidden unless certain conditions are fulfilled.[3] Such regulations can result in higher costs, reduce economic opportunities, close markets, and restrict access for consumers to new products and services. These are discussed in more details in Section 3.2 below.

A balance needs to be struck between facilitating the smooth flow of data while at the same time preserving privacy, protecting individual and public safety, and promoting national security. As governments assert national sovereignty over online content and products, they must also respect the legitimate interests and sovereignty of other jurisdictions and recognize the critical importance of access to an increasingly global network of cloud services for businesses large and small. We encourage NTIA to further work with USTR and the Department of State to help advocate the following steps that governments can take to address these challenges in its international engagements:

- Minimize adverse impacts on products or services that involve cross-border data transfers,
- Encourage e-commerce, which invariably involves cross-border data flow, refrain from imposing customs duties or other taxes on cross-border electronic transmissions (consistent with the 1998 World Trade Organization (WTO) moratorium on e-commerce duties), and commit to extending nondiscriminatory treatment to digital products and services,
- Ensure that legislation provides maximum flexibility and creates the least risk of conflicting national rules,
- Adopt trade commitments that foster data-driven innovation.

1.2 Freedom of Expression Online

When considering the removal of user content from cloud services, it is important to distinguish between: (1) government laws, order or actions to remove content; and (2) cloud service providers' removal of content in order to maintain the nature and purpose of the service and meet the needs and expectations of users (e.g., through terms of use, code of conduct, or community guidelines for the service).

In the case of government laws, order or actions to remove content, international human rights laws have long recognized the human right to freedom of expression. It is a key contributor to human dignity and the development of human potential. Of course, any technology, whether the printing press or the cloud, can

[2] Manyika, J., and Chui, M., "By 2025, Internet of things applications could have $11 trillion impact," Fortune, July 22, 2015.

[3] Ferracane, M., "Restrictions to Cross-Broder Data Flows: a Taxonomy," European Center for International Political Economy, November 2017.

be misused to disseminate illegal or harmful content. This raises important questions for governments, communities, cloud service providers and other stakeholders, who seek to ensure freedom of expression, and the right to receive and impart information on the global internet while protecting public safety. As societies seek to protect human rights while combating content such as terrorist or extremist content, it is important to recognize that public safety and human rights are complementary values that reinforce each other.

As appropriate, NTIA should endeavor to work collaboratively with the Department of State and enhance awareness with other relevant U.S. government agencies to help advocate for governments to adopt clear laws and regulations that protect public safety, freedom of expression and other human rights – all of which are critical to the digital economy. In particular, governments should consider the following principles:

- *Adhere to the rule of law in regulating online content.* Such laws and regulations and their enforcement must be transparent and respect international human rights laws and norms. Citizens should be engaged in their enactment as well as enforcements. The rule of law also requires that enforcement orders and decisions be subject to independent judicial approval and review, with meaningful and trusted opportunity for companies and individuals to appeal judicial approvals or decisions.
- *Adopt a principled approach to online content regulation that protects freedom of expression and other human rights as well as public safety.* Any governmental restriction on freedom of expression should respect the norms established by international law – namely, legality, necessity, and proportionality. Restrictions should be the least restrictive means possible and should be proportionate to the legitimate objective.
- *When removal of online contents is demanded, enact laws and regulations that are transparent, narrowly tailored, sufficiently detailed and clearly define what constitutes illegal content and the types of services that must remove it.* When governments demand that online service companies remove content, they should do so transparently, through legal orders that are specific, narrow and detailed to enable companies to identify precisely which content must be taken down. Such laws and legal orders should not require companies (directly, or indirectly through intermediary liability or other pressures) to proactively monitor content or make independent determinations of illegality. Laws and regulations should not restrict companies from informing the public about removal demands from governmental authorities.
- *Respect national sovereignty through international cooperation and adhere to international norms when considering content regulation on the global internet.* Where existing rules or processes for cross-border cooperation are outdated or cumbersome, governments should work together to update them so they keep up with new technologies, are adequate to address new challenges and protect human rights.
- *Avoid interference with technology companies' terms of use*. Companies generally provide processes for users or others to report content that may violate the terms of use and have procedures for review and removal of content that violates applicable terms of use.

Relevant organizations and forums for the U.S. government to engage in to support, promote and advocate for the free flow of information and freedom of expression include:

- The United Nations, specifically the Office of the UN High Commissioner for Human Rights , and the UN Special Rapporteur on the right to freedom of opinion and expression,
- The Freedom Online Coalition, a partnership of 30 governments, working to advance internet freedom. Coalition members work closely together to coordinate their diplomatic efforts and engage with civil society and the private sector to support internet freedom – free expression, association, assembly, and privacy online – worldwide, and

- The Global Network Initiative, a multistakeholder organization that addresses freedom of expression and privacy rights of internet users in the context of government demands for content restriction or user data in the information and communication technology (ICT) sector. Its members consist of ICT companies, civil society groups, academia, and investor groups.

1.3 Cross-Border Domain Takedown Requests

As pressure increases on the need to address online abuses across borders, the number of requests sent to technical operators to suspend cross-border domain names that are associated with illegal content or activities has been increasing. Such measures have global impact and need to be undertaken carefully. There must be strong and agreed-upon procedures in place to ensure proportionality in any response. The Internet & Jurisdiction Policy Network has identified two different types of abuses that give rise to domain name suspension requests: (1) abuses that leverage the Domain Name System (DNS) itself, including phishing, diffusion of malware, or support for botnets; and (2) site content or activity that is considered illegal or harmful, including distribution of child abuse images, illegal online pharmaceutical sales, counterfeiting or copyright infringement.

Both types of abuse may involve operators, domain holders and users in multiple jurisdictions, where consideration of national laws is required. These cases often raise issues regarding applicable laws, and the lack of recognized international legal frameworks render court decisions difficult and untimely as a mechanism to resolve these types of issues. This is compounded when content or activity may be considered legal in one jurisdiction and illegal in another.

ICANN has a role in addressing some of these challenges, as part of enforcing the obligations in the accreditation contracts for registries and registrars. Through its engagement on ICANN's Governmental Advisory Committee (GAC), NTIA should remain vigilant to developments in which actors attempt to leverage concerns over these very real cyber threats to impose inappropriate limits on freedom of expression through domain name suspension policies or process.

2 Multistakeholder Approach to Internet Governance

2.1 Importance of Multistakeholder Approaches

Multistakeholder approaches, where business, government, civil society, the technical community, and other stakeholders participate equally, have driven development of the internet and enabled tremendous socio-economic progress in using ICT to bridge the digital divides globally. Microsoft supports continuing the use of inclusive, open, transparent, bottom-up multistakeholder approaches to internet governance public policy development. Governments need to work with other stakeholders to create appropriate policy and regulatory frameworks to enable continued innovations on the internet and sustainable economic development, especially in support of the UN Sustainable Development Goals (SDGs). As mentioned previously, Microsoft has partnered with local business, governments, civil society, and others in numerous projects around the world to bridge the digital divides and connect the 4.4 billion people who are still unconnected – both are high priorities for us. We partner both on the supply side – through initiatives such as Airband; as well as on the demand side – building capacity for the local community to adopt, produce, and consume localized content and services safely though training for all people, particularly youth, girls, disadvantaged populations, and support for local small- and medium-sized enterprises.

Multistakeholder is the optimal approach in development of policy frameworks where innovation in technology, business models, and markets is evolving quickly, such as those involving the internet, digital transformation, and emerging technologies such as AI. As these can pose challenges to existing regulatory frameworks, stakeholders including government, business, civil society and academics need to work together to identify policy and regulatory approaches that can best realize the potential of the innovation while mitigating the challenges. Through open dialogues, stakeholders can identify and prioritize potential socio-economic and regulatory challenges, and share responsibility on how to best mitigate these challenges by leveraging their respective unique expertise. It is essential that technological innovation be considered as part of such solutions.

A balanced policy approach that includes a combination of self-regulations, voluntary- and market-driven technology standards, sharing of best practices, application of existing regulations, and where appropriate, updated policy and regulatory frameworks, needs to be considered. In its international engagements, NTIA should coordinate with other agencies to continue to advocate for such balanced approaches as well as multistakeholder involvement in the development of holistic policy and regulatory frameworks that are focused on sustained investment and inclusive economic growth.

2.2 ICANN Priorities

1) IANA transition

Microsoft relies on the stability, resilience and security of the DNS system to enable our cloud services, and the IANA functions are critical to the operation of the internet. Microsoft welcomed the transfer of the stewardship over the IANA functions from NTIA to the global multistakeholder community as a significant and necessary development. The transition is a recognition of the value and success of the multistakeholder approach which has guided the evolution and exponential growth of the internet, and its contribution to global GDP. Microsoft sees no reason to “unwind” the IANA transition; indeed, such action would undermine the essence of the multistakeholder approach to internet governance and should therefore be avoided.

The IANA transition needs to be fully completed, principally via efforts being made to improve ICANN’s accountability mechanisms, and we note the progress being made by ICANN’s Cross-Community Working Group (CCWG) on Accountability. ICANN needs to continue to be held accountable to the multistakeholder model, and we are confident that the conclusion to the Accountability CCWG’s work will help ensure this happens.

2) WHOIS compliance with the General Data Protection Regulation (GDPR)

WHOIS is the authoritative source for the contact and technical information of registered domain name registrants. With the enactment of the GDPR, there are compliance issues for WHOIS in how this information is shared and who can have access to it. Microsoft believes privacy is a fundamental human right and we embrace the GDPR. We also believe in the critical importance of maintaining a stable and secure internet, which is central to ICANN’s mission. Based on existing consensus policies and contracts, ICANN is responsible for “implementing measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information”, subject to applicable laws.[4] Registrars and registries must provide information for the WHOIS service as part of their agreements with ICANN.

Microsoft sees no conflict between GDPR compliance and the use of WHOIS data for legitimate and important purposes such as cybersecurity. Indeed, there are references in the GDPR explicitly foreseeing the validity of processing data for security purposes. Since Reverse WHOIS is the single most useful tool Microsoft has for identifying cybercriminals and disrupting their operations and is vital for enabling us to

[4] https://whois.icann.org/en/primer.

protect our company, our customers, and the public at large, it is essential that this legitimate purpose be correctly defined and maintained.

However, the unique position of the ICANN organization as a joint data controller not in possession of the data being regulated has led to that organization seeking to create legal clarity for the community-at -large to create policy within its multistakeholder model. To that end, the Temporary Specification adopted by ICANN on May 17 has been used to collect feedback from data protection authorities (DPAs) and as a starting point for developing subsequent policy. Microsoft believes that the Temporary Specification goes further than is necessary and proportionate in its efforts to bring WHOIS into compliance with GDPR and has led to a fragmentation of the WHOIS system as registrars and registries take divergent approaches, due to the document's lack of definitions – e.g., what constitutes providing "reasonable access" to WHOIS data. We also view the Temporary Specification as an incomplete compliance model as it does not include mechanisms for uniform approaches to accreditation, authentication and access to data for legitimate purposes under the GDPR.

The June 18 publication of a framework for a Unified Access Model was a positive first step by ICANN and a welcome sign that it is intent on completing the compliance model. However, the development and implementation of an access and accreditation solution must be treated as an urgent priority, and solutions – even if temporary – must be implemented as they become available.

We urge NTIA to continue to engage with ICANN to contribute to efforts to define permanent, practical, efficient and predictable solutions to bring WHOIS into compliance with GDPR, resulting in a mandatory, uniform access and accreditation solution as soon as possible, ensuring that: users with legitimate purposes under the GDPR can have persistent and frictionless access to WHOIS data without requiring users to be validated for each individual request; contracted parties cannot redact the non-personal data of legal persons (whose definition includes companies and organizations that are outside the scope of the GDPR); there remains the ability to analyze data in ways that are crucial for cybersecurity professionals to be able to act swiftly and strategically to disrupt cybercrimes, including the continued possibility to conduct Reverse WHOIS searches or consult current and historical WHOIS data in an aggregated fashion.

2.3 Improvements to the IGF

Since its inception at the Tunis phase of the World Summit on the Information Society (WSIS) in 2005, the IGF has been a leading platform for multistakeholder dialogue on issues of importance to internet governance. The IGF has been remarkably successful in fulfilling its mandate as articulated in paragraph 72 of the Tunis Agenda, and by "providing an open and inclusive multistakeholder platform to address policy issues relate to the internet."[5]

We acknowledge the various efforts that have been devoted to the review and continuing improvement of the IGF's structure and agenda, including the recommendations of the CSTD Working Group on Improvements to the IGF and the WSIS+10 review. The progress report by Ms. St. Amour, as delivered to the CSTD twentieth session, is an excellent accounting of the progress that has been made in meeting the recommendations of the CSTD Working Group on Improvements to the IGF. Among the ongoing efforts by the IGF to address the CSTD recommendations, we would particularly applaud the noticeable improvements in the preparations for the annual meetings and the expanded use of technology that has increased transparency and inclusiveness of these processes, as well as contemporaneous availability of transcripts and webcasts from sessions.

[5] Lynn St. Amour, Chair of the Multistakeholder Advisory Group, statement at United Nations Commission on Science and Technology for Development (CSTD) twentieth session, 8-12 May, 2017, Geneva.

There are areas for continuing improvement to the IGF, to further strengthen its role as a leading platform for multistakeholder dialogues on issues related to internet governance. However, in considering improvements, it is important to maintain the IGF's original intent, as stated in paragraph 72 of the Tunis agenda and as refined in the subsequent years, including the WSIS+10 Outcome document. As input to this NOI, we identify the four areas below. We look forward to continuing to work with NTIA, the Department of State, other appropriate U.S. agencies and other government sponsors to address these issues.

1) *Drawing on existing strengths and outputs to increase impact for the IGF*

Some have called for the IGF to produce more concrete outputs and outcomes. Microsoft believes that it would be a mistake to look for more concrete outputs in a way that would turn the IGF from a platform for non-binding multistakeholder dialogues on policy issues into a negotiating forum and dilute the energy that currently enables such rich exchanges of views.

Indeed, Microsoft's current Airband initiative to enable broadband connectivity and energy access to underserved communities can be traced directly back to a meeting at the 2011 IGF in Nairobi. That meeting led to the creation of Project Mawingu to deliver low-cost wireless broadband access to previously underserved locations near Nanyuki, Kenya. Since then, the TV White Space technologies underpinning that project have been deployed through trials and commercial deployments in more than 30 countries; and the systems integrator involved in Project Mawingu has evolved into a fully-fledged commercial ISP whose business model is being regarded as a reference for other African countries. These are the types of meaningful and impactful outcomes that are enabled by the IGF platform as it was designed.

In addition, the IGF produces many written outputs, ranging from reports from the intersessional work to summaries of discussions at the annual meetings. The intersessional efforts (e.g., Best Practice Forums, Connecting the Next Billion and the Dynamic Coalitions) allows discussions and sharing of best practices; they are particularly effective at localizing the IGF dialogue on key issues on internet governance. The annual meetings provide a vibrant venue which enables participants to learn new perspectives and build connections between people and organizations. More can be done to consider how these written outputs could be better presented, organized, and made more accessible and searchable. This would improve the impact of the IGF, enable better leverage of past work, and gain a wider audience for the valuable work it does. For example, a rich repository of easily browsable and searchable materials on the IGF website can be created by compiling outputs from the IGF sessions at each annual meeting.

2) *Developing and implementing a multi-year plan towards 2025*

The IGF is now in the third year of the 10-year renewal provided for by the WSIS+10 review in 2015. We believe that the IGF needs to be more focused on addressing the areas for improvement identified in the WSIS+10 Outcomes document, to show demonstrable progress by 2025. To do this, it should develop and implement a multi-year plan that provides more continuity and works towards meeting the goals set out in the WSIS+10 Outcome document. Ideally, the multi-year work program should be organized and approached in a step-by-step manner, allowing the IGF to prioritize and focus on achieving a select set of prioritized goals every year.

In this context, we welcome a proposal being considered and developed in the IGF Multistakeholder Advisory Group (MAG) Working Group on Multi-year Strategic Work Program which proposed a comprehensive review of where the IGF processes have worked well and where there is need for further guidance and decision-making by the MAG. This work should result in a common action plan with defined processes and responsibilities and frameworks for decision-making, in line with improvements suggested by the CSTD Working Group on IGF.

3) Stabilizing funding of the IGF

There have been continuing uncertainty and shortfalls in the IGF budget which has inevitably impacted stability for its annual program, as well as activities of the secretariat, whose dedication and excellent support have always been exemplary, despite the constant shortage of resources needed.

This shortfall can be addressed either by increasing the number of donations, the amount of individual donations or, in the commendable example of the Government of the Netherlands, by pledging a multi-year annual donation. At present, fundraising relies on the efforts of the MAG Chair and volunteer MAG members. The IGF should consider the principle of returns on investment by investing in short-term professional assistance (e.g., a consultant with fundraising expertise) to expand the pool of donors and extend the amount of multi-year pledges.

We urge NTIA to work with others and the IGF to explore the possibility of securing financial assistance from the UN. We understand that, by design, although the IGF is bound by the administrative rules of the UN, it does not receive any funding via the UN beyond in-kind support for use of UN facilities such as at the 2011 IGF in Nairobi and the 2018 IGF in Paris. Alternatives to extend UN financial assistance to the IGF, which would provide the IGF with a stable underpinning to its budget, should be explored.

4) Addressing the declining engagement of governments and the private sector

We have seen an unfortunate decline in government and private sector attendance at the annual meetings – between 2014 and 2017, government attendance fell from 23.8% to 20.3% of all attendees, and private sector attendance from 24.2% to 14.6%. This trend risks leading to an imbalance that needs to be addressed as a factor in the long-term sustainability of the IGF. It is not a simple problem to address, but there are a number of ways forward which could help improve the situation. For example, improved packaging and marketing of the Forum's existing outputs could help to clarify and increase awareness of the activities and goals of the IGF, and its relevance to these stakeholders. National and Regional IGFs might be well-placed to reach out to national governments and business, encouraging them to participate in the local and then annual meetings.

3 Privacy and Security

3.1 Cybersecurity

Microsoft welcomes NTIA's statements in the NOI about the importance of cybersecurity to economic growth and innovation. Microsoft shares NTIA's view that strong, industry-led cybersecurity risk management practices should be at the core of multilateral dialogues about cybersecurity policy, and NTIA's efforts to promote this approach within APEC, IGF, and OECD are helpful. Microsoft also appreciates the opportunity to have served as lead contributors in NTIA's multistakeholder processes for cybersecurity policy issues, including the development of the recent recommendations to increase security transparency for IoT consumers. Going forward, we encourage NTIA to continue to partner and coordinate with industry stakeholders as it pursues security priorities identified through this process.

In its international advocacy role, NTIA should encourage governments and international organizations to leverage cybersecurity risk management practices that reflect industry experience and have proven successful across sectors and around the world. In February, the International Standards Organization (ISO) and International Electrotechnical Commission (IEC) issued a technical report, Information technology - Security techniques - Cybersecurity and ISO and IEC Standard (ISO/IEC 27103:2018), that articulates a helpful framework for enterprise cybersecurity risk management. The structure and guidance provided in the report, which built on the widely-used US National Institute of Standards and Technology (NIST) Cybersecurity Framework by integrating many more relevant ISO and IEC standards, demonstrate how public and private sector organizations can effectively develop and implement their cybersecurity risk management programs. The report should inform policy and regulatory measures to set cybersecurity baselines, or minimum organizational and technical measures, focusing limited resources on effective practices and driving greater interoperability among sectors and across the global environment. Moreover, NTIA should partner and coordinate not only with industry but also with other groups that are pursuing related and potentially reinforcing initiatives within Commerce, including the International Trade Administration (ITA) and NIST.

Consistent with NTIA's commercial perspective on cybersecurity, Microsoft also encourages NTIA to leverage its platform and roles in international organizations to call attention to the economic impact of cyber-attacks. Earlier this year, nearly 40 technology companies committed to the Cybersecurity Tech Accord, which reflects industry's concern about the impact of nation-state attacks on technology users. Likewise, the WannaCry and NotPetya attacks of 2017 demonstrated that highly-connected enterprises can suffer hundreds of millions of dollars in losses when cyber-attacks take down their operations. Indeed, the UK National Health Service's assessment of WannaCry's impact on its systems illustrated how cyber-attacks have the potential to disrupt the ability of institutions to perform basic functions, like provision of medical care. As the escalating trend of nation-state cyber-attacks creates the risk of greater costs in the future – both to economies and human beings themselves – NTIA, and other relevant agencies, should support efforts in international fora to work towards greater nation-state restraint in cyber-attacks.

3.2 Privacy Considerations and Interoperability of Frameworks

Privacy is a business imperative for Microsoft and one of our three core pillars; the others being cybersecurity and ethics.[6] As a provider of tools and platform services to empower people, we can only succeed if our customers deem our technologies sufficiently trustworthy to use them broadly. Individuals are concerned about the privacy and security of their digital information and (foreign) government access to this information. Companies need regulatory certainty to continue investing in cloud services and realize the full potential of cloud computing. Establishing trust has been an integral part of our operation and our DNA for decades – we pioneered the industry's first Trustworthy Computing initiative in 2002 grounded in four key areas – Security, Privacy, Reliability, and Business Integrity – which have only increased in importance since.

As a global corporation, we need to comply with relevant local privacy laws and regulations. The GDPR enacted by the European Union is a significant development in data protection law, and Microsoft is committed to complying with the GDPR. We are investing in the largest engineering effort that we have ever undertaken to satisfy a regulatory requirement to meet this commitment.

We firmly believe that a strong legal framework for data protection provides an essential foundation for data-driven innovation and entrepreneurship to flourish. Such foundation should integrate the following core principles to instill the level of trust needed to propel international trade, sustain economic growth and create new opportunities for everyone inclusively:

[6] Satya Nadella, Keynote at Build, May 7, 2018.

- *Requirements should apply to all types of entities that process personal data, i.e., data that is identified or reasonably identifiable to an individual, including employees*. This is similar to the definition of *personal data* under GDPR and comparable legislation worldwide. However, data protection rules that apply to the public sector should include meaningful restrictions on data processing to demonstrate that the law provides essentially equivalent protection to data protection laws in other regions to facilitate the free flow of data across borders. Appropriate restrictions on data processing by the public sector are also important for fostering the trust of foreign data subjects whose data may be accessed by the local government.
- *Consumers should be granted data subject rights that are at the heart of GDPR*, including:
  - (i) Know what data is collected about them and the purpose for which data is processed,
  - (ii) Receive an electronic copy of the personal data collected,
  - (iii) Request rectification of inaccurate personal data,
  - (iv) Delete personal data, subject to certain exceptions, including that companies should be permitted to retain data if there are "overriding legitimate grounds for the processing" (e.g., security purposes) or when necessary for compliance with a legal obligation (e.g., laws mandating certain retention periods).

  Microsoft has already extended the rights at the heart of GDPR to all our consumer customers worldwide.
- *A distinction should be maintained in defining responsibility for a data controller, which determines the means and purposes of processing data, and a data processor, which processes the data on behalf of another organization.* Liability should be allocated among organizations that process data according to their agreement, or barring an agreement, then according to demonstrated fault giving rise to the liability.
- *Processing of personal data should require strict standards for consent or other legal grounds for processing*. The GDPR includes a provision allowing processing that is necessary for legitimate interests, performance of a contract, compliance with a legal obligation, or tasks carried out in the public interest, which must be demonstrated through rigorous, documented analyses of privacy risks and mitigations. Laws should expand the concept of legitimate interest to incorporate the possibility of new purposes for processing previously collected data that may not have been knowable at the time of collection, but that are compatible and appropriate with the original purposes of processing, subject to rigorous documentation of the privacy risks and mitigations. For example, processing data in the AI context should be enabled when a company engages in robust pseudonymization of data, conducts a thorough, documented assessment of the impacts and risks associated with the data processing, and documents and implements safeguards and accountability measures to minimize the identified impacts and risks.
- *Processing of sensitive personal data should not be broadly restricted*. Rather, the level of restriction on the processing of personal data should correspond to the context in which the data is processed**.**
- *Use of data that has been subject to de-identification techniques that either eliminate or reasonably reduce the ability to connect data with a specific individual should be promoted.* The commitment to not reidentify the data should apply both to the controller of the data and to any other entity to whom the controller provides the data.
- *Overly broad extraterritorial application of data restrictions should be avoided.* Such restrictions create challenges for compliance and enforcement, and risk hampering innovation and growth for both domestic industry and companies with global operations. Sweeping application of such laws may create a reciprocity effect which may impede the ability of domestic companies to operate internationally, as well as restrict the level of business which could get sent to local companies for data processing or analysis. Where national security necessitates access to personal data and cross-border data flows, compliance with international agreements, such as Mutual Legal Assistance

Treaties (MLATs) is critical when data that raises specific privacy risks is to be shared with law enforcement organizations in third countries. Microsoft supports efforts to improve upon current bilateral and multilateral government data sharing agreements.

- *Intercompany and cross-border data flows that are protected through appropriate technical and legal measures should be facilitated, and the location of data should not be prescribed.* While often well-intentioned, cross-border transfer restrictions and data localization measures can be difficult to implement, damage the economy, and unable to address the primary privacy concerns associated with data processing. More effective approaches can be leveraged that can also help to improve resiliency and security and make data processing services more efficient by reducing latency. Examples of these approaches include:
  - Existing bilateral or multilateral frameworks that enable companies to use established principles and mechanisms to protect the privacy and security of personal data as it moves across borders (e.g., the EU-U.S. Privacy Shield can be used as a model for other jurisdictions).
  - Data transfer agreements consistent with EU standard contractual clauses should be recognized as acceptable mechanisms for maintaining accountability and legitimizing cross-border transfers.
  - Certification to industry codes of conduct that are developed through open, multi-stakeholder processes enables companies to show their compliance, including through certifications to international standards such as ISO/IEC 27001/27018/29100.[7] These standards are effective ways of addressing privacy and security concerns associated with emerging technologies and rapidly evolving business models.
  - Alignment with the OECD "Accountability Principle" enables data to be transferred across borders if the data controller remains accountable for protecting the data regardless of its geographic location.

  Recognition of the above programs across borders, such that a given mechanism can be used in multiple markets, would provide consistency for regulators and customers evaluating companies' compliance, while not being overly bureaucratic.

  We also encourage the addition of provisions on data flows in international trade agreements. Such commitments have the virtue of being enforceable, and under industry's preferred formulation, would include a "necessity test" that is assessed by an independent third party (vs. self-judging) for any proposed barriers. Multilateral agreement on rules to ensure cross-border data flows at the WTO would be ideal; including such provisions in bilateral and plurilateral trade agreements is also valuable.
- *Notices of security breach should not be required in cases that do not threaten real harm to the individuals involved.* The GDPR excludes from notification requirements breaches that are unlikely to result in a risk to the rights and freedoms of individuals. Over-notification may engender "notification fatigue" or detract needed resources and regulators focus from material breaches. Notices should be made without undue delay, and not be given a prescriptive timeframe.
- *Special consent requirements should apply at least for children under the age of 13, aligning with current U.S. practices*. It should be permissible to process children's data when doing so is necessary to comply with a legal obligation or to guard the health or ensure the physical integrity of the child.
- *Laws should be as technology-neutral as possible as technologies, e.g., cloud, artificial intelligence, will continue to quickly evolve.*

[7] ISO/IEC 27001 provides guidance on organization information security risks; 27018 provides guidance for the protection of personally identifiable information by cloud service providers acting as processors; 29100 provides information on a privacy framework.

- *A data protection framework should be applied consistently to different industries, with oversight from a central regulator that has broad understanding of different industry sectors, rather than distributing the responsibility amongst several regulators.*

Microsoft believes that robust privacy protections do not have to, and should not, stifle innovation. It is important to consider the consequences of regulations that are being proposed, or in some cases implemented, and be willing to examine the impact on innovation and make modifications as necessary – multistakeholder dialogues are essential in these processes. Appropriate privacy regulations can be critical for establishing a trusted environment and lead to even greater prosperity for U.S. companies. For example, although the GDPR creates new challenges for AI, some of the GDPR's core principles (accountability, transparency, fairness) can be leveraged to create greater trust in human-centered AI systems and enable broader adoption. The OECD's revised Privacy Principles from 2013 is another such set of principles. For this reason, as the OECD undertakes an effort to review these Guidelines starting in 2019, it is essential that NTIA works with business to provide input into the process to ensure that emerging technologies such as AI are considered in the revision, and that the review will be evidence-based.

Privacy is an essential pillar for enabling the digital transformation. We urge NTIA to consider the above tenets in its work on privacy principles and in its participation in the OECD review of the Privacy Principles. This review can also serve as good indicators on whether broader agreements on cross-border data flows are possible. NTIA should also work closely with other agencies focused on commercial and trade issues in international forums, including the European Commission, APEC, the OECD, and the WTO, to address the issues raised above, to coordinate and present consistent U.S. government positions that can strongly endorse holistic policy and regulatory frameworks that are focused on sustainable investment, economic growth and innovation.

4 Emerging Technologies and Trends

4.1 International Venues for Policy Development on Emerging Technologies and Trends

After decades of relatively slow progress towards fulfilling the promise of digital transformation, recent advances in computing are making that promise real. And businesses large and small are at the forefront of the digital transformation**,** leading with innovations that foster sustainable growth both globally and locally. As technologies move at a faster pace than rules and regulations are made and implemented, it is important that governments not impede the future by regulating the past. Business input is essential to the development of policy and development of holistic policy and regulatory frameworks for inclusive and sustainable growth.

As global economies become even more interconnected, governments are increasingly turning to multilateral organizations and international forums to promote their agendas more broadly. At the same time, these dialogues are merging, and the respective forums are evolving. Microsoft believes that no single multilateral organization has the competency or mandate to address all aspects of policy development for issues related to the internet or digital transformation, and that there needs to be an ecosystem of organizations with a variety of expertise, experience, and activities working in a coordinated manner, leveraging and building on each other's strength. Within this ecosystem, it is more important than ever to remind multilateral organizations of their unique historical mandate and expertise – to avoid duplication and inefficiencies. But each organization, properly managed, has much to offer. It is, therefore even more important for governments, in cooperation with the multistakeholder community, to find the best ways to develop constructive and evidence-based policies, based on recommendations and decisions from multilateral organizations.

Within the ecosystem of international organizations addressing policy topics related to the digital transformation, the ITU and the OECD stand out. The ITU is a leader in harmonizing public telecommunications networks and global use of radio spectrum. Technical considerations are important for maintaining a safe, secure, resilient, and globally interoperable infrastructure and platform. The OECD is a leader in developing policy recommendations and principles that are focused on sustainable investment and inclusive economic growth, using approaches that are based on evidence, economic modeling and statistical analysis. Each has much to offer, separately and together, and each can make significant contributions to the vital importance of telecommunications, the internet, and digital transformation in enabling global innovation, inclusive growth, creating new opportunities, education, and improving civic and cultural life. However, each organization has a specific remit as established in its founding and governing articles. When organizations expand beyond their mandates and engage in work that is already being done elsewhere, the lack of expertise and appropriate context can lead to these activities being done in a silo, rather than as part of an integrated and holistic policy framework that is focused on enabling sustainable investment and inclusive growth – issues that are critical to bridging digital divides and creating healthy digital ecosystems. When work is duplicated, this can also create confusion and dilute core competencies.

Of note is that the OECD is one of the few multilateral organizations where business can participate in policy development, and where business input is sought. The OECD is well-respected for its evidence-based policy recommendations that have shown, in many instances, positive influences on national regulations. For example, its Privacy Guidelines, established in 1980 and updated in 2013, serve as the basis for many national data protection regulations worldwide, including the GDPR. Business, through the Business and Industry Advisory Committee (BIAC), has been working hard to be a strategic partner in the OECD Going Digital project launched in 2017. The project leverages the expertise of 14 OECD committees to develop a coherent and comprehensive policy approach, guidelines and toolkits for governments.

The latest OECD working draft on an "Integrated Policy Framework" for its Going Digital project described a holistic enabling policy and regulatory framework that is whole-of-government and whole-of-society, and requires consistent policy approaches across sectors and policy silos, all aimed at achieving sustained investment, economic growth, and societal well-being.[8] This OECD project is the only policy framework for digital transformation that explicitly includes the different policy silos, showing that achieving inclusive growth and well-being requires appropriate balance between the silos. With the OECD being the Secretariat for the G7 and G20, we urge U.S. government representatives to promote this integrated policy framework approach in these international forums to help shape the respective declarations to be more amenable to business needs.

Microsoft very much appreciates NTIA making the issues surrounding "multilateral organizations" one of the questions addressed by the NOI. With the increasing interconnectedness of global economies and the proliferation of duplicative activities related to the development of relevant policies – in silo in a lot of cases – serious considerations are needed on the role of multilateral organizations writ large, the role of different multilateral organizations within an ecosystem and how multistakeholder approaches can constructively contribute to the development of holistic policy and regulatory frameworks that enable sustained investment, innovation and inclusive economic growth globally. We urge NTIA to work with the Department of State and other appropriate agencies to ensure that U.S. business interests are strongly

[8] Directorate for Science, Technology and Innovation, Committee on Digital Economy Policy, "Going Digital Integrated Policy Framework for Making the Transformation Work for Growth and Well-being," 24 April 2018, DSTI/CDP/GD(2018)5.

represented in these forums, and to shape the work in these organizations so that they are coordinated, not duplicative, in ways that are consistent with their mandates, core competencies and experience.

Furthermore, a balanced policy approach should include a combination of self-regulations, technology standards, sharing of best practices, application of existing regulations, and where appropriate, updated policy and regulatory frameworks. As the number of technologies grow, globally interoperable standards that are voluntary and market-driven play an increasingly essential role in policy frameworks as well as form the bases for market efficiencies. Where applicable, NTIA should support efforts from NIST and business organizations in developing these standards and specifications in open, voluntary, consensus-based standardization bodies and industry-led, market-driven standardization initiatives with multistakeholder input. Active business participation and input in standardization efforts will usually result in market-driven approaches that consider actual needs as well as practical implementation concerns.

In its international engagements, NTIA should coordinate with other agencies to continue to advocate for such balanced approaches as well as multistakeholder involvement in the development of these policy and regulatory frameworks.

4.2 Artificial Intelligence

Microsoft firmly believes in the potential of AI to empower and create new opportunities for every person and every organization. AI works by searching for patterns in large training data sets and using these patterns to make predictions or recommendations. Defined as such, AI is "computational intelligence" that enables new advances in nearly every field and progress in many existing societal challenges when it is used by subject matter experts. As a company that develops platforms and tools, our vision on AI is that it should be human-centric, that it augments human ingenuity to enable advances in every human endeavor.

For AI to be adopted and deployed on a global scale, its development needs to be shaped to foster trust and broad adoption. This can be realized only if relevant stakeholders from business, government, civil society and the research community can work together on shared principles and ethical frameworks. In January 2018, Microsoft released the book "The Future Computed: Artificial Intelligence and its role in society," to contribute our perspectives to this global dialogue and encourage a sense of shared responsibility that we all have in shaping this development. We believe that commitment to the principles of fairness, reliability and safety, privacy and security, inclusiveness, supported by an underlying foundation of transparency and accountability provide a solid framework for building trust and should guide the development of AI.

We are actively working with other companies, academics, and civil society, as well as governments globally on these issues. The Partnership on AI to Benefit People and Society (PAI), launched in late 2016, was part of this effort. PAI's mission is to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society. Today, PAI has more than 50 partners from 9 countries, more than 50% of whom are non-profit.

Based on the OECD's past work, its focus on the economic context, and its evidence-based approach, Microsoft strongly endorses its initiative on development of human-centric AI policy and its efforts to develop principles that will enable trustworthy development and deployment of AI systems around the world. Any such output would also be relevant to all governments. Its work thus far, including the AI conference on "Intelligent Machines, Smart Policies" in 2017 and initial draft paper on "Artificial Intelligence in Society Phase 1," is unique in the thoughtful, comprehensive and balanced way in which it examines the topic and the current status of development of the technologies.[9] We appreciate that the OECD is proceeding carefully and exploring evidence in its efforts to develop AI principles, and support its efforts to establish an expert working group to scope principles to foster trust in and adoption of AI in society. For these reasons, we urge NTIA, and more broadly the U.S. Government to give strong support to the OECD efforts on AI as well as the Going Digital project, and furthermore, to establish the inter-agency consensus necessary to take strong leadership roles in shaping these activities.

The ITU efforts in AI include its convening of the AI for Good Summit (2017, 2018), expanded work items on AI in the ITU-T Study Group 3, the ITU Focus Group on Machine Learning for Future Networks including 5G, and AI-related activities at WTSA-16. The ITU should seek to focus its AI work on its core mandate, while also avoiding inefficient and costly duplication of existing work on AI, such as that at the OECD; the Institute of Electrical and Electronics Engineers (IEEE); the AI standards initiatives at the International Organisation for Standardization; the Partnership on AI; 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. The ITU's role and value add within the ecosystem of organizations working on AI should be further explored through multistakeholder consultations and dialogues, including considerations on 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.

Technical standards specifications on AI are essential components of an overall AI policy framework. The newly formed ISO/IEC subcommittee on AI met for the first time this April to discuss some fundamental building blocks, including a reference architecture for AI, standardized terminology and concepts, and study groups that address computational approaches and characteristics of AI systems, technical standards solutions to trustworthiness of AI, and use cases of AI. NTIA should work with NIST to promote this work more broadly as it is laying some much-needed foundation for the current dialogues on AI, including consistent definitions and terminologies.

AI technologies are being widely perceived as game changing economically and politically. PwC has estimated that by 2030, AI can increase global GDP by 14%, or $15.7 trillion, and that almost half of these economic gains will accrue to China, where AI is estimated to boost the economy by 26% over the next 13 years or $7 trillion in GDP.[10] AI is expected to bring about the largest increase in GDP for North America in the next few years as consumers and industries are more ready to incorporate AI, however, China will rise to the top in the mid-2020's. With governments around the world expressing increasing interest in AI, and especially in establishing regulatory and ethical frameworks, we urge NTIA, and more broadly the U.S. Government to actively engage in shaping the development of AI policy frameworks domestically as well as globally to preserve U.S. leadership and competitiveness in this important area.

The development of AI technologies that are human-centric and policy frameworks that benefit from multistakeholder collaboration and are evidence-based need to be promoted. As AI is still at a nascent stage of development, an open dialogue between government, business, civil society and academic researchers is essential to shaping the continued development of the technology and realizing its potential

[9] Directorate for Science, Technology and Innovation, Committee on Digital Economy Policy, "Artificial Intelligence in Society Phase 1," 27 April 2018, DSTI/CDEP(2018)9.
[10] PwC, "What the real value of AI for your business and how can you capitalise?" June 27, 2017.

benefits. Working together, we can identify and prioritize issues of societal importance as AI evolves, enable sharing of best practices and motivate further research and development of solutions as new issues emerge. Policy discussions should aim to promote broad development and deployment of AI across different sectors and continued AI innovation, encouraging outcomes that are aligned with the vision of human-centered AI. We believe policymakers should:

- Continue to convene broad dialogues among government, business, researchers, civil society and other interested stakeholders on how AI can be shaped to maximise its potential and mitigate its risks, including adoption of practical guiding principles to encourage development of human-centred AI,
- 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, making more government controlled and funded data sets available to enable broader experimentation with AI and comparisons of alternative solutions to address ethical concerns.

4.3 Online Content, Applications and Services

There is a symbiotic and self-reinforcing positive relationship between the networks underlying the internet and the applications, content, and services accessed by means of those networks. A holistic policy framework needs to consider the value of the entire internet ecosystem for the internet to remain a platform for innovation, competition, and sustainable economic growth, not only today, but also in the years to come. There is evidence that compelling content and services drive increased demand for broadband internet access. For example, a WIK study found that broadband networks in Europe benefit significantly from increased bandwidth demand driven by incremental use of applications, and specifically that "higher demand (and potentially willingness to pay) are key in enabling profitable investment and reducing risks for telecommunications providers."[11] A more recent study concluded that services that facilitate rich interactions among users "generate a significant component of the socioeconomic impact of the digitization of the internet itself."[12] Because of the increased demand for broadband and data connections, traditional network operators benefit significantly from consumer demand for the edge offerings that are delivered over the internet.[13] Conversely, online content, application, and service providers remain critically dependent on more and better broadband internet connections to their customers. The untethering of features and services from physical networks has only strengthened the interdependent and synergistic relationships between applications and networks.

The realm of online content, applications, and services should be embraced as part of a holistic framework for enabling investment and inclusive growth. Instead, some governments and multilateral organizations have approached the regulatory debate by arguing that there is a need to "level the playing field," usually by applying legacy, traditional telecommunications regulations to online content, applications, and services.

[11] WIK, "Applications and Networks: The Chicken or the Egg, the Role of Digital Applications in Supporting investment and the European Economy," March 2, 2015.

[12] WIK, "The Economic and Societal Value of Rich Interaction Applications (RIAs)," May 2017.

[13] CTIA, Wireless Snapshot 2017.

We urge NTIA to continue its support of the critical role that online content, applications, and services play in the entirety of the internet economy and the benefits they produce, and reject the notions advanced by some that online content, applications, and services "free ride" on access networks. Microsoft appreciates the work NTIA has done on this issue, for example in ITU-T SG3 and ITU-D SG1. In these and other forums, NTIA should continue to advocate against reflexively extending legacy regulation to the world of online content, applications, and services, and for eliminating barriers that can adversely impact the evolution of the internet ecosystem. The pace of change in the way the world interacts continues to accelerate, driven by fundamental shifts in the technology of communications networks, the capabilities offered over those networks, and the relationships between those networks and capabilities. Regulation, meanwhile, rarely evolves at the same velocity as technological progress. Thus, national regulators must look forward to where markets and technology will be and not just where they are now. Such foresight is necessary to determine whether current regulations remain fit for purpose, new regulations are necessary, as well as the potential impact of such regulations on enabling sustainable growth of national digital economies.

Conclusion

Microsoft appreciates the opportunity to provide this response to assist the NTIA in prioritizing policy issues for international engagements that relate to the internet, internet-enabled economy, and more broadly, the digital transformation of economies globally. We especially appreciate NTIA's recognition of the importance of international engagements to maintain U.S. competitiveness and leadership in these challenging times. This response provides further compelling evidence of this need, and, we hope, sufficient guidance for NTIA, where it has authority. Where it does not, we urge NTIA to help advocate, on our behalf, that the Department of Commerce, other relevant agencies, and more broadly the U.S. government, prioritize these issues in their respective international engagements. Microsoft looks forward to continuing to engage with NTIA on these issues.

Respectfully submitted,

MICROSOFT CORPORATION
Paul Mitchell, Senior Director
Internet Governance
3460 157th Avenue NE, Redmond, WA 98052
(425) 706-9064

M-H. Carolyn Nguyen, Director
Technology Policy
901 K Street, NW, Washington, DC 20001
(202)831-6475
cnguyen@microsoft.com