DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

International Internet Policy Priorities

Docket No. 180124068–8068–01

COMMENTS OF AT&T SERVICES, INC.

Robert C. Barber
James Wade
David Lawson
AT&T Services, Inc.
1120 20th Street NW
Suite 800
Washington, D.C. 20036
(202) 457-2121 (phone)

July 17, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW Room 4725
Washington, DC 20230
Attn: Fiona Alexander,
iipp2018@ntia.doc.gov

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

AT&T[1] welcomes the Department of Commerce ("DOC") and the National Telecommunications and Information Administration's ("NTIA") Notice of Inquiry ("NOI" or Notice")[2] on International Internet Priorities seeking to identify important issues facing the internet globally. AT&T respectfully submits these comments regarding such challenges and offers recommendations to NTIA regarding the optimal direction of its resources and policy expertise to respond to stakeholders' priorities and interests.

AT&T is an integrated media and entertainment company providing mobile, video and data solutions. AT&T operates one of the world's most advanced backbone networks. As of 2Q2018, we carry more than 206 petabytes of data traffic on an average business day across our network to nearly every continent and country. We have experienced an increase in mobile data traffic on AT&T's national wireless network of more than 360,000% between 2007 and 2017, with smartphones driving almost 75% of our data traffic in 2018. With operations throughout the U.S. and in over 60 other countries, AT&T has extensive experience as a fixed line operator and a wireless operator, serving individual consumers and the world's largest enterprises, in the dynamic areas of converged technologies and services. Given our global presence as both a network operator and content provider, we have a unique window into the important multiplier effect that Information and Communications Technology ("ICT") services have across other economic sectors and the important role ICT services play stimulating the economy.

[1] AT&T Services, Inc. submits these comments on behalf of itself and the other affiliates of AT&T, Inc. (collectively, "AT&T").

[2] Vol. 83, No. 108 Fed. Reg 26036 (June 5, 2018)

The United States Government (U.S.G.) – led by the DOC (through the NTIA), along with the Department of State, and the FCC -- has historically been uniquely positioned to play an important leadership role in helping shape international internet priorities and to use that position to work with stakeholders across the global ecosystem to establish a comprehensive, coherent, and consistent policy framework that will promote the continued success of the Digital Economy worldwide. Indeed, this Administration has recognized that the ‘‘[t]he flow of data and an open, interoperable internet are inseparable from the success of the U.S. economy,’’ and has unequivocally reaffirmed that ‘‘the United States will advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services.’’[3]

We urge the U.S.G. to continue to leverage its unique position to lead the development of evolving and emerging policies that further these important goals. To that end, AT&T offers these comments underscoring: (i) the importance of promoting interoperable frameworks that will remove barriers to the free flow of information; (ii) the benefits of U.S.G. leadership to multilateral and multi-stakeholder engagement; (iii) the need to promote flexible privacy and cyber security policies that protect consumers and foster the growth of the global digital economy; and (iv) the benefits of investment in emerging technologies.

[3] Executive Office of the President, *The National Security Strategy of the United States of America* (Dec. 2017), *https://www.whitehouse.gov/wpcontent/ uploads/2017/12/NSS-Final-12-18-2017- 0905.pdf, note 4.*

I. NTIA SHOULD ENCOURAGE THE FREE FLOW OF INFORMATION BY PROMOTING INTEROPERABLE FRAMEWORKS AND REMOVING BARRIERS TO THE FREE FLOW OF DATA.

As NTIA has previously recognized, cross-border data flows are essential to the global digital economy.[4] The World Bank, the McKinsey Global Institute, and others have also documented the ways in which cross-border data flows permit the creation of global value chains, allow small and medium enterprises to participate in the global economy, and give consumers the benefit of a greater variety of products and services.[5] Conversely, there is little evidence that policies that hinder the free flow of data – such as requirements for local storage of data -- produce tangible benefits for local economies.[6]

Governments can build trust in the global economy by creating an environment for service providers to follow industry best practices and guidelines regarding the cross-border use and protection of personal data, while providing appropriate accountability mechanisms for those who wish to challenge data management practices. Positive examples of accountability-based frameworks that facilitate the cross-border flow of data include agreements such as the APEC Cross-Border Privacy Rules (CBPR) Framework, the OECD Privacy Framework, the Privacy Shield, and the EU-US Principles for ICT Services. AT&T commends the U.S.G.'s efforts to promote the CBPR and the OECD Privacy Framework, as well as to negotiate a robust EU-US

[4] See, e.g., U.S. Department of Commerce, *Measuring the Value of Cross-Border Data Flows* (September 2016).

[5] See, e.g., World Bank, *World Development Report 2016: Digital Dividends*, available at: http://www.worldbank.org/en/publication/wdr2016; McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, 6 (2016), available at: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age; International Chamber of Commerce, *Trade in the Digital Economy: A primer on global data flows for policymakers* (September 2016), available at: https://iccwbo.org/publication/trade-in-the-digital-economy/.

[6] Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Information Technology and Innovation Foundation (2017).

Privacy Shield and other data transfer mechanisms, as these frameworks represent widely accepted international standards for the collection, use, and transfer of personal data which contain accountability mechanisms for individuals and state actors who wish to challenge data management practices.

Stable and interoperable cross-border privacy frameworks are extremely important to AT&T and our customers. In today's Digital Economy, almost every business has an online presence and a need to exchange data internationally with customers and other businesses. Political or legal uncertainty regarding the ongoing availability of cross-border transfer mechanisms creates significant operational and financial challenges for businesses and their customers. This disruption of cross-border data flows has far-reaching economic consequences and threatens to impede the continued growth of the Digital Economy.

We recommend NTIA engage other agencies of the U.S.G. to promote effective frameworks to ensure that the cross-border transfer mechanisms in which the United States participates are easily accessible to any U.S. company that seeks to benefit from them. Efforts to make the APEC system and EU data protection rules interoperable have the potential to benefit industry and digital trade, but there are opportunities to do more. For example, experts have suggested that the APEC CBPR system could be opened to non-APEC economies or even possibly transferred to a secretariat that is independent of APEC, allowing it to operate on a global level. This is a possibility worthy of serious exploration. The U.S. government can strengthen both the APEC CBPR framework and Privacy Shield by encouraging the participation of other U.S. agencies in these arrangements.

In addition to the international venues identified above, the U.S.G. should continue to engage on digital privacy issues with the International Conference of Data Protection and Privacy

Commissioners and the Global Privacy Enforcement Network. International coordination on privacy enforcement issues is an effective way to address concerns about cross-border data flows and to demonstrate the U.S. commitment to strong consumer protections. The FTC should continue to be sensitive to the concerns of international regulators and to pursue aggressive enforcement against companies that have failed to comply with the rigorous requirements of the Privacy Shield.

International trade agreements also are valuable mechanisms for safeguarding the free flow of data and bolstering the digital economy. The United States – European Union Trade Principles for ICT Services[7] and the provisions of the Trans-Pacific Partnership's concerning cross-border data flows[8] are positive examples of such agreements. We support the continued joint promotion of the former with the EU and the inclusion of similar E-Commerce provisions from the latter in future bilateral and multilateral trade agreements.

NTIA should also support efforts to engage with states that may take aggressive approaches to obtaining data stored beyond their borders when it is related to criminal and national security investigations. While the United States and its allies work to clarify the legal regime applicable to

[7] On April 4, 2011, the U.S. and EU announced agreement on a set of non-binding trade-related principles for information and communication technology (ICT) services, including: "2. Open Networks, Network Access and Use: Governments, preferably through their regulators, should promote the ability of consumers legitimately to access and distribute information and run applications and services of their choice. Governments should not restrict the ability of suppliers to supply services over the internet on a cross-border and technologically neutral basis, and should promote the interoperability of services and technologies, where appropriate; 3. Cross-Border Information Flows: Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries."
https://ustr.gov/sites/default/files/uploads/agreements/morocco/pdfs/2011-04-04%20ICT%20principles%20text%20FINAL.pdf

[8] Trans Pacific Partnership, Chapter 14, Electronic Commerce, Article 14.11: Cross-Border Transfer of Information by Electronic Means, "1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."

cross-border data requests, NTIA and other agencies should continue to promote respect for the integrity of digital security technologies. The integrity of digital technologies is indispensable to protecting the privacy and security of individuals, businesses, governments, and civil society around the world. Both consumer and enterprise customers expect that their sensitive information will be protected by and will remain within the control of the business from which they are obtaining products and services. At the same time, we recognize the legitimate role of law enforcement agencies in protecting public safety and national security, and the need for legal regimes to respond to technological changes through fair, accountable and uniform procedures that govern when and how private companies may be compelled by the government to provide information. This important policy issue should be subject to robust public debate and addressed in legislation, so that it is implemented in a consistent and transparent manner.

The Clarifying Lawful Overseas Use of Data (CLOUD) Act[9] is a positive step toward addressing this challenge, but it is important that the bilateral agreements and rules that implement it clearly establish the circumstances under which public authorities may issue demands for personal information, the forms that such demands must take, and the specific authorities that are empowered to make them. Companies should be permitted to challenge demands that appear inconsistent with the legal framework in court. NTIA and other U.S.G. agencies should engage proactively with the European Union and with other parties to the Council of Europe Convention on Cybercrime as these bodies propose approaches that complement the CLOUD Act, such as the European Union's e-Evidence proposal.[10]

[9] **H.R. 1625**: Consolidated Appropriations Act, 2018.

[10] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

In addition to these efforts, the U.S.G. should strive to improve Mutual Legal Assistance Treaties (MLATs) and similar processes. MLATs will serve as the primary means for providing access to data for states that do not have executive agreements with the United States and for situations in which the CLOUD Act does not clearly provide for a direct request to a provider.

II. MULTI-STAKEHOLDER AND MULTILATERAL ORGANIZATIONS ARE STRENGTHENED BY CONTINUED NTIA, U.S.G. AND INDUSTRY ADVOCACY AND ENGAGEMENT.

AT&T is dedicated to the continued development of an open, highly secure, and interoperable global internet that fosters social and economic development for all people and supports the long-standing multi-stakeholder approach for internet governance development. The internet is a globally distributed network of networks -- no one party, company or government "owns" it. As a result, a decentralized and international multi-stakeholder system for governance, drawing upon the expertise of all stakeholders, remains necessary for internet growth and expansion. As the internet has evolved and grown, so too has the multi-stakeholder model of internet governance. Successful multi-stakeholder engagement aligns with the following principles:

- Processes are open, inclusive, transparent, and accountable and enable all relevant stakeholders to participate, engage, and contribute to the discussions and decision-making;
- Participants should work to ensure a shared understanding among stakeholders of the issues and a desire to collaborate to address the issues.
- Local stakeholders (civil society, individuals, academia, local government and local business) should be involved in a meaningful way to provide expertise, grass-roots level input and to raise awareness about cultural sensitivities.

Active engagement among service providers, governments, users and other stakeholders is the single most effective way to address legitimate concerns about unlawful and harmful internet information flows, while at the same time ensuring a balanced and narrowly tailored process that promotes the paramount human rights, privacy and commercial interests of users to exchange information and ideas on the internet. We urge the U.S.G. to continue its support for fora that provide critical leadership in the discussion of best practices on a range of emerging issues, including cybersecurity capacity building, broadband infrastructure deployment, and enabling policy frameworks in developing nations.

The Internet Governance Forum (IGF) is an example of a multi-stakeholder platform in which U.S.G. engagement is important. The IGF, established by the Tunis Agenda in 2005, is a global multi-stakeholder and multilateral platform where all stakeholders participate on equal footing with the objective of gathering and sharing information and expertise and developing voluntary best practices and guidance on a range of internet-related matters. The recent decline in representation from key governments and high-ranking officials at the IGF has reduced its influence and perceived relevance to other stakeholders. NTIA should work with other branches of the U.S.G. to encourage the participation of U.S.G. officials and of other leaders in the digital economy to enhance IGF discussions and strengthen the IGF's ability to lead meaningful discussions and help shape the policy landscape. The IGF should also be encouraged to select venues for meetings that are economical and to establish adequate funding and other resources to ensure its long-term viability.

We also encourage the U.S.G. to remain engaged in other multi-stakeholder efforts that affect internet governance. AT&T participates in several ICANN constituencies and remains committed to helping ensure that ICANN is not unduly influenced by any government that would either jeopardize the free and open nature of the internet, or improperly apply geo-political decisions to internet management. We encourage NTIA and other U.S.G. agencies to remain engaged with ICANN to ensure ICANN remains committed to the principles of:

- Supporting and enhancing the private sector-led, multi-stakeholder model;
- Maintaining the security, stability, and resiliency of the internet Domain Name System;
- Meeting, with accountability, the needs and expectation of the global customers and partners of the IANA services;
- Maintaining the openness of the internet;
- Remaining free from government control.

Further, we encourage NTIA to help ICANN swiftly resolve the perceived barriers presented by GDPR that have resulted in the limitation of access to the WHOIS system. The move from an open, publicly available WHOIS service to an approach requiring a layered and restricted access model for WHOIS is making it costlier and more time consuming for legitimate rights holders to act against infringers and bad actors, including those responsible for malware, botnet attacks, phishing schemes and other attacks. WHOIS should be preserved as a key tool in the ongoing fight against cybercrime, malicious actors, and intellectual property infringement.

Multilateral organizations serve an important role as platforms for the exchange of information and best practices, capacity building efforts, and awareness-raising of issues and opportunities to engage in existing multi-stakeholder efforts. Any discussions undertaken in multilateral fora effectively must continue outside a multilateral government-led organization to ensure the ongoing vibrancy and speed of internet evolution. Moreover, any related policy development and technical work should be undertaken by multi-stakeholder organizations with the expertise and mandate to carry out such activities. This model is not always easy, but for more than twenty years, it has delivered an enviable record for promoting expansion of services across geographies, and NTIA's (and the entire U.S.G.'s) continued commitment to and engagement in that model is critical to continuing that trend.[11]

III. NTIA SHOULD PROMOTE RISK-BASED CYBERSECURITY FRAMEWORKS THAT ARE ALIGNED WITH NATIONAL AND SECTORAL CYBERSECURITY AND PRIVACY FRAMEWORKS THAT BALANCE CONSUMER PROTECTION AND INNOVATION.

A. Voluntary, Risk-Based Cybersecurity Frameworks Will Promote Risk Mitigation and Digital System Security to the Benefit of the Digital Economy.

We live in a connected world where individuals use multiple communication devices and services from different providers. Digital networks are globally linked and malicious actors in the digital environment are not constrained by national borders. Thus, as more industries push to "go digital," (e.g. manufacturing, agriculture, healthcare), cybersecurity and trust in ICT systems become essential components of international commerce. In this environment, cybersecurity and resulting trust in systems is an enabler of economic activity.

Prescriptive and fragmented regulatory approaches to cybersecurity threaten to become trade barriers and to divert resources towards compliance and enforcement avoidance (without necessarily improving actual security), rather than to security programs tailored to risk. Promoting

[11] Indeed, significant progress has been made over the past decade to connect the unconnected and to enable access to information and knowledge for all people. For example, the number of internet users has tripled over the last ten years, from 1 billion to over 3 billion today. Most of this has been accomplished because of light-handed government policies with regard to the internet, which has actively promoted private sector investment, innovation, and competition as the engine to drive consumer connectivity. Despite these and other gains, we recognize more work remains to deliver the benefits of the internet and ICTs to all corners of the world, and we remain committed to do our part to help achieve these shared goals. While some parties support a greater role for governments – or a government-only top-down approach – in the policy, technical, and commercial aspects of the internet, the U.S. should seek to preserve the existing model that acknowledges the important role of all stakeholders and is predicated on bottom-up, consensus-based decisions.

adoption of aligned, voluntary cybersecurity risk management frameworks via trade discussions and agreements (and independent of such) will promote risk mitigation and digital system security, thereby increasing trust in digital systems.

We urge NTIA to continue its work across the U.S.G and with the private sector and civil society to develop policies that encourage the continued development of a U.S. strategy for global coordination to address cybersecurity issues and to promote international commerce. A coordinated U.S. strategy designed to shape the international environment is key as nation states grapple with how to best address threats that are not confined by national borders such as, for example, the emerging concerns with the security of the Internet of Things (IoT). Bringing together like-minded nations for discussion on a host of issues, such as technical standards, flexible security frameworks, acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force is a critical part of mitigating the growing cybersecurity threat.

Further, cybersecurity as an industry is rapidly growing. Global spending on cybersecurity is estimated to reach more than $170 billion by 2020. Policies designed to facilitate and streamline international trade in the cybersecurity industry will foster continued growth, continued innovation, and promote employment in an industry where technical expertise in the workforce is acutely felt globally.

B. NTIA Should Promote Privacy Frameworks Based on the Principles of Choice, User Control and Security, Making Companies Accountable Through Self-Regulation Without Being Prescriptive.

To make data-driven innovation compatible with data privacy, it is critical to empower users without over-regulating data controllers or data collection. The public policy focus should be on providing regulatory certainty and consistency, supporting the principles of choice, user control and security, and making companies accountable through self-regulation without being prescriptive. The framework should recognize that market/industry driven developments have led to an increase in user transparency and trust. Further, privacy rules should be consistent across the global digital ecosystem. Privacy regulations that apply to only one set of technologies, data class or industry players can create confusion. Rather, consumers expect that one set of common rules will apply to the processing of personal data, regardless of whether a device manufacturer, an application provider, or a connectivity provider does the processing.

NTIA should collaborate with other U.S.G. agencies to build consensus around the adoption of federal baseline privacy legislation in the United States. A clear legal framework will demonstrate U.S. leadership in this area and provide a model for other states. It will also facilitate the operations of companies that may be obligated to comply with a patchwork of requirements in different U.S. states. Although the development of the NIST Framework has proven successful in the area of cybersecurity, the interest of consumers in exercising greater control over their personal data and the disparate approaches to regulation that some U.S. states have pursued justify a federal legislative approach to privacy.

IV. EMERGING TECHNOLOGIES AND TRENDS WILL THRIVE IN AN ENVIRONMENT WHERE THE GOVERNMENT AND PRIVATE SECTOR WORK IN TANDEM TO DEVELOP A RISK-BASED POLICY FRAMEWORK.

Several emerging technologies are re-shaping industries' and consumers' use of the internet around the world. Chief among these trends are the continued development of the IoT, and the advent and nascent deployments of 5G networks. Ongoing international coordination amongst stakeholders, to include NTIA and other U.S.G. agencies, will help ensure that these technologies can deliver on their promises to internet users domestically and around the world.

A. Internet of Things

The developments in IoT technologies and the global spread of IoT business largely have been achieved in the absence of, and not because of, government oversight and intervention. The innovation that has fueled the explosive growth in IoT technologies to date has been the result of private sector investment, in a climate of slight, if any, regulatory oversight. Accordingly, it is vital for NTIA to advance a policy framework internationally that will support the continued, aggressive investment in the next-generation network infrastructure necessary to power the IoT. Over-regulation of communications networks will slow the deployment of the ubiquitous, next-generation networks over which the IoT will ride as it develops over the coming years.

Such an international framework should first prioritize the voluntary, industry-driven efforts that have already fostered such successful growth for the IOT. Where there are industry best practices or voluntary frameworks already in place, the governments should respect and support them. Where new standards or policies are necessary to address evolving issues, rather than moving immediately to prescriptively regulate, governments can encourage—and, in some cases convene—multi-stakeholder initiatives as the first step in addressing issues associated with newly emerging IoT applications or technologies. But NTIA should encourage international policymakers to resist the temptation to reactively prescribe a "solution" for these issues that risks artificially skewing the development of the market or technology development. Instead, regulators should let competition, innovation, and customer demand drive developments in the IoT marketplace.

While an increasingly connected world continues to change our lives for the better, the security of such devices and the data that they send and receive has become critically important. In 2015 there already were approximately 25 billion connected devices. By 2020, that number is expected to double, with estimates of up to 50 billion "things"— from wearable and implantable medical devices to sensors in cars, traffic lights, utility meters and household appliances—sharing data over IP connections.[12] The breadth of devices is also staggering—from smart cities to connected cars and homes, to medical devices, to utilities management to the manufacturing sector, connected devices increasingly benefit our day-to-day lives. IoT devices communicate with each other, to back-end servers, and to cloud infrastructure. These devices need to be identified, authenticated and allowed secure access to resources. The wide distribution of IoT devices to consumers and industries alike trigger diverse and immense new security challenges (as demonstrated by recent high-profile IoT-related attacks) and present an opportunity for cybersecurity innovation.

Policymakers around the world are grappling with how to best address security challenges posed by and to the IoT, as evidenced in emerging discussions around certification schemes,

[12] See James Manyika et al, Unlocking the Potential of the Internet of Things, McKinsey & Co. (June 2015), http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world. The potential economic value of these devices will be measured in the trillions of US dollars. In fact, as noted in the request for comments, one study estimated that the cross-sector impact of IoT could be as much as $11 trillion—approximately 11 percent of the global economy—by 2025. *Id.* at 2 and 101 (calculating a "low end" economic impact of $3.9 trillion for IoT, and describing the barriers to achieving the "high end" of $11.1 trillion).

frameworks, and regulation. As policy efforts take shape around the world, we encourage NTIA to promote collaborative policy development and implementation that includes government, and industry, and avoids regulatory and legislative solutions that are overly prescriptive. While certification frameworks can play an important role in IoT security, legislation or regulations – such as those that would set static security requirements and certifications for devices surrounding updatability and vulnerability disclosures -- would risk turning IoT security into a checklist regulatory environment that promotes meeting a bare minimum over providing the most secure solutions. Moreover, these approaches run the risk of becoming quickly outdated—a particular concern for changes made by statute given the pace of the legislative process. We urge the NTIA to work with the Department of State to undertake an effort, comparable to that undertaken in developing the NIST Cybersecurity Framework, to develop an IoT Security Framework. Global industry has already led the way here, as evidenced by the recent announcement of the adoption of the GSMA IoT Security Guidelines and Assessment by network operators around the world—including AT&T.[13] NTIA's international support and encouragement for industry-led efforts like this can help promote a global interoperable security framework for the IoT.

Another international policy challenge facing the IoT is the regulatory permissibility of device numbering resource utilization across regions and countries. As we noted in our comments to NTIA's NOI on the Advancement of the Internet of Things in 2016,[14] regulators around the world must allow IoT service providers (and network operators) to use the numbering resources and device provisioning methods most suitable to the IoT use cases, rather than applying mobile phone / smart phone based regulatory regimes on IoT services using mobile networks. NTIA

[13] https://www.gsma.com/newsroom/press-release/gsma-global-mobile-operators-commit-to-common-approach-to-iot-security/

[14] Comments of AT&T Services, Inc. in Docket No. 160331306-6303-01, June 2, 2016.

should thus promote the development of standards and operating frameworks for the effective global deployment of IoT solutions.

Other emerging technologies will present similar challenges for policymakers in coming years. Of note, the President's National Security Telecommunications Advisory Committee (NSTAC) produced a comprehensive report on emerging technologies last year.[15] That report outlined and made recommendations for developing strategic policy plans for emerging technologies such as software defined networks, quantum computing and identity management.

B. 5G Networks

As NTIA is well aware, the global race to 5G is well underway.[16] 5G brings with it many exciting use cases (and many use cases are not known today) focused on the capabilities that 5G will deliver – a promise of greater speeds and more responsiveness (lower latency). These attributes are critical for applications ranging from 4K video, augmented and virtual reality, real-time gaming, smart homes and cities and so much more. It also means connected devices and unleashing the real potential of the IoT, indeed massive IoT. 5G also promises greater sophistication in network traffic management. This is important for enabling controls such as network slicing, which allows the operation of multiple virtual networks over common infrastructure allowing network resources, including spectrum, to be used much more efficiently.

The industry has been planning, trialing, testing and moving 5G technology from the lab to real-world experimentation over the last couple of years. Along the way, standards bodies have been taking this information and have already set standards for significant aspects of 5G. Indeed,

[15] NSTAC Report to the President on Emerging Technologies, May 18, 2017, *available at* https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20ETSV%20Report%20Executive%20Summary%20508%20Compliant_1.pdf.

[16] *See, e.g.,* Remarks of Assistant Secretary Redl at CTIA's Race to 5G Summit, April 19, 2018, *available at* https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-ctias-race-5g-summit.

just a month ago the 3GPP and its contributing members reached another milestone on the path toward 5G networks: the close of the Release 15 standards development and freeze of Rel. 15 specifications. This will allow global industry stakeholders to continue towards the rapid deployment of standards-based 5G networks in the coming months and years—while 5G standards development within 3GPP will continue through work on Release 16. Even as standards continue to develop many companies have announced plans to begin deploying 5G this year. AT&T has announced an aggressive timeline to deploy standards-based mobile 5G to customers in 12 markets by the end of 2018 and have shared the first three markets where we'll deploy this year – parts of Dallas, Atlanta, and Waco. For our launch, service will be over millimeter wave spectrum and we're using the 3GPP non-standalone configuration from release 15 standards. This means our deployed 5G radios will run on our LTE core. This integration means customers can pass between a 5G service area to LTE with a seamless handoff between the two technologies.

To realize this 5G vision, the industry needs additional spectrum and they need the ability to efficiently, timely, and cost effectively place additional infrastructure, including small cells. These core needs have been recognized by NTIA, the FCC, and Congress who have done an outstanding job in raising awareness and moving the ball forward. The U.S.G. can continue this momentum and play an important role at the ITU World Radio Communications Conference 2019 (WRC-19) in advancing 5G by supporting the allocation of additional spectrum for mobile broadband use.

The U.S.G. should likewise help promote spectrum policies globally that will promote investment and help enable 5G deployment globally. The explosion of IoT combined with the continued evolution of 4G LTE and the advent of 5G are also driving investment in other new technologies like network function virtualization (NFV) and software-defined networking (SDN), which are replacing traditional communications infrastructure. New 5G millimeter-wave spectrum and associated technologies will further drive innovative use cases, along with the 5G Next Generation Core network which embraces software and automation as the foundation of future telecommunication networks. The combination of these technologies is moving industry in the direction of 5G, with the vision of enabling a high speed low latency wireless network to essentially do what a fixed network can do today.

CONCLUSION

The mobile internet and high-tech innovation that catapulted America to global leadership in innovation were the direct outcome of deliberate and wise government policy established more than 20 years ago. Beginning in the 1990s, policymakers agreed, on a bipartisan basis, that light-touch regulation was the proper approach for the internet. This decision helped unleash more than two decades of remarkable innovation and competition, across the U.S. internet ecosystem, rooted in equally remarkable levels of investment.

Indeed, the U.S. broadband industry overall has invested more than $1.4 trillion since 1996. Over the past 5 years (2013-2017), AT&T alone invested more in the U.S. than any other public company: nearly $145 billion in our wireless and wireline networks, including capital investments and acquisition of wireless spectrum and operations. This historic level of investment was a result of regulation that looked forward, not backward.

AT&T applauds the DOC and NTIA for undertaking this important inquiry into identifying both the key challenges to International internet governance and the appropriate approaches for the successful governance of the internet. The DOC and NTIA are particularly well-positioned to take a leadership role in developing a forward-looking global policy framework that will ensure the continued growth of the digital economy supported by light-touch regulatory models and effective multi-stakeholder engagement. AT&T looks forward to continuing working with the DOC, NTIA and other stakeholders in that important work.

Respectfully submitted,

/s/ Robert C. Barber
Robert C. Barber
James Wade
David Lawson
AT&T Services, Inc.
1120 20th Street NW
Suite 800
Washington, D.C. 20036
(202) 457-2121 (phone)

July 17, 2018