POLICY PRIMER: AN OVERVIEW OF 5G DEPLOYMENT, STANDARDS, AND SECURITY

Executive Summary

5G is critical to the future of the U.S. economy. Larry Kudlow, Director of the National Economic Council, recently discussed figures released by CTIA and Accenture estimating that 5G is poised to add $500 billion to the nation's GDP and 3 million new jobs. The United States must lead on 5G.

The United States is currently winning the global "race" to 5G, and all four national carriers have announced plans to provide 5G service between late 2018 and mid-2019. AT&T is poised to lead on 5G, and we plan to be the first company to introduce mobile 5G service based on industry standards, starting with twelve cities this year and seven more cities in early 2019.

The government can help ensure the U.S. advantage through sensible policies. Eliminating regulations and barriers to deploying small cells is crucial, and we applaud the FCC's recent actions on this topic. Likewise, smart spectrum policy will help ensure the timely availability of spectrum assets for commercial use.

AT&T has prepared white papers on key 5G topics – deployment, standards, and security. Below are the key takeaways from these important topics.

The Competition-Based Industry Model in the United States Is Winning the Global "Race" to 5G.

- 5G will be the most robust wireless communication technology deployed to date and will enable faster and more powerful networks. 5G is an evolution of technology, not an overhaul.
- All four major U.S. carriers will provide 5G services between late 2018 and mid-2019, and nearly half of the mobile subscriptions in North America will be 5G by 2023. Carriers in China, on the other hand, are still trialing 5G technology this year.
- The U.S. government bolsters the U.S. advantage on 5G through policies that reduce obstacles to wireless deployment, such as the FCC's recent framework for small cell permitting and the FCC's plan to make additional low-, mid-, and high-band millimeter wave spectrum available for 5G services. The United States already has more spectrum available for 5G than any other country, and the government's light-touch regulatory approach will continue the momentum on 5G deployment.

China is not winning the "race" to 5G because it has the most cell sites per square mile and per person. More important than raw numbers are the characteristics of tower sites, the geographic realities of areas being covered, and the amount and band of available spectrum.

Some mistakenly believe that China dominates 5G because its companies have made the most "contributions" to 3GPP, the global standards organization for 5G. The raw number of contributions reveals little. Many contributions are supported by other members. And there is no "quality-control" for submissions, so not all initial contributions are of equal merit, and some contributions are duplicative. Finally, contributions do not automatically become part of a specification; they must go through a rigorous consensus process. **U.S. carriers have been leading in open, transparent, and collaborative standards work**.

The Global Standards Process Is Robust and Effective in Advancing U.S. Goals.

- Global standards are critical for interoperability between networks and devices. Standards foster the economies of scale needed for global development of new technology.

- The global telecommunications ecosystem has a history of collaborating on standards. This is not a government-driven process. It is left to private experts—engineers, scientists, and other builders—to debate problems and solutions, working toward consensus in a transparent way.
- AT&T wouldn't have committed to launch standards-based mobile 5G in 2018 if we weren't completely comfortable with 3GPP's work. 3GPP operates under detailed procedures to ensure regional balance and transparency. No country, region, industry segment, or company can dominate 3GPP's activities or its outputs.
- All countries and companies must wait for the same standards to be developed to manufacture equipment and deploy 5G. Any non-standard deployment will not be scalable or interoperable with other networks.

Future Wireless Networks Will Have Unprecedented Security.

Some believe the move of 5G to the edge will make networks less secure. To the contrary, network virtualization, edge computing power, device management, and automated threat detection and response will create **more flexible and secure networks**.

- Several innovations in network design and wireless technology will intersect to create a highly secure and resilient 5G network. We will have more agile and layered security as we transition from centralized core and radio access networks to distributed, virtual networks.
- 5G technology introduces a new network segment, the Mobile Edge, which includes elements traditionally part of the Radio Access Network (RAN) and Mobile Core. As critical functions migrate to the Mobile Edge, carriers are implementing new and embedded security functionalities to ensure a highly secure mobile network, including:
    - Distributed Denial of Service (DDoS) detection and mitigation at the edge of the network to enhance the ability to respond to attacks and reduce potential broader network impact.
    - Stronger encryption for over-the-air interface and encryption of each device's IMSI to further secure device consumer-specific information.
    - A Security Edge Protection Proxy that will mitigate vulnerabilities in prior technology (e.g., SS7 and Diameter) and attacks when subscribers are roaming between different carriers' networks.
- In addition, wireless providers are increasingly deploying network components that are virtual instead of relying on the hardware of the past. As network operations are virtualized, through Network Functions Virtualization (NFV) and Software Defined Networking (SDN), 5G's virtual and cloud-based network systems will allow for more adaptable security because they can be quickly adjusted, removed, or replaced using software, reducing the likelihood that an entire network would be impacted by a cyberattack.

These white papers provide an overview of three critical topics facing future wireless networks: the pace of deployment, standards, and security. Policymakers and others interested in the future of wireless communications should review them to understand how the U.S. private sector is building the foundation for the future digital economy. Policymakers should protect the U.S. commitment to a regulatory environment that promotes bottom-up innovation so that the United States can remain the global leader in technology.