REMARKS OF FCC CHAIRMAN AJIT PAI
AT THE FCC FORUM ON 5G OPEN RADIO ACCESS NETWORKS

SEPTEMBER 14, 2020

Good morning, and welcome to the FCC's Forum on Open Radio Access Networks. This event originally was scheduled for March. But I hope and expect that it will be worth the wait.

Thank you all for joining us, and special thanks to all our conference participants. We have quite the lineup today. All 5 FCC Commissioners will be speaking. We have many experts representing world-leading technology companies and upstart firms. We have top talent from the academy. We have Commerce Department Director of Policy and Strategic Planning Robert Blair. We have former Ranking Member of the House Intelligence Committee Jane Harman, who now leads the Wilson Center. And, for the first time I'm aware of, the U.S. Secretary of State is participating in an FCC event.

Usually, the Commission could only get a turnout like this by offering free food. Clearly, that is not the case here. So what's the big deal?

The big deal is 5G. These next-generation wireless networks will be embedded in almost every aspect of our society and economy—from businesses to homes, hospitals to transportation networks, manufacturing to the power grid.

Over the past few years, the FCC has aggressively executed our 5G FAST plan to secure American's leadership in 5G. This strategy features three key parts: freeing up commercial spectrum, promoting wireless infrastructure, and encouraging fiber deployment.

This strategy has yielded significant results. For example, we've completed multiple spectrum auctions that have repurposed huge swaths of spectrum for 5G. And we've seen record-breaking capital investments in infrastructure essential for next-generation networks.

But our focus isn't limited to promoting networks that are strong. We're also committed to making sure that they are secure.

For years, U.S. government officials have expressed concern about the national security threats posed by certain foreign communications equipment providers. To address this concern, we've aimed to protect the integrity of the communications supply chain—that is, the process by which products and services are manufactured, distributed, sold, and ultimately integrated into our communications networks.

Specifically, the FCC has prohibited the use of money from our Universal Service Fund to purchase or obtain any equipment or services produced or provided by companies that the Commission determines pose a national security threat, namely Huawei and ZTE. We also initiated a process to identify and catalog insecure equipment used in USF-funded communications networks so that we can hopefully implement a program to remove and replace it once Congress appropriates funds for this purpose.

Looking to the next generation of wireless technology, much of the equipment at the heart of 5G networks currently comes from just a few global suppliers. Three of the most prominent are Sweden's Ericsson, Finland's Nokia, and South Korea's Samsung, but the largest of them is the Chinese company Huawei.

Carriers building out 5G networks rightfully worry that Huawei equipment could expose them to security risks. Huawei's market power, aided by generous subsidies from the Chinese Communist Party, often might seem to make that company the cheapest and thus best option for network equipment. But the Chinese National Intelligence Law requires companies like Huawei to cooperate with, and keep secret, State intelligence work. The law also creates opportunities for Chinese intelligence agencies to

compel access to an organization's facilities, including communications equipment, in certain cases. In short, many are recognizing that you get what you pay for, and that the long-term costs of using insecure equipment are likely to outweigh any short-term savings.

In addition to these security issues, carriers may be concerned by a relatively consolidated marketplace. Some have told me, both here and abroad, that vendor diversity is useful in terms of price competition, avoiding the lock-in problem, and ensuring a backup supplier, among other things.

Technological innovation has opened up a new path to address these concerns. That technology is the subject of today's forum: Open Radio Access Networks, or Open RANs.

Open RANs could transform 5G network architecture, costs, and security.

Traditionally, wireless networks rely on a closed architecture in which a single vendor supplies many or all the components between network base stations and the core. But Open RANs can fundamentally disrupt this marketplace. We could see an exponential growth in the number and diversity of suppliers. We could see more cost-effective solutions. And critically, we could see the keys to security in the hands of network operators, as opposed to a Chinese vendor. All this may explain why some telecom companies are beginning to develop and deploy open, interoperable, standards-based, and virtualized radio access networks.

As an added bonus, many of the leading firms in the Open RAN space are based in the United States or in countries generally aligned with our vision of 5G security.

How this marketplace will evolve is hard to predict with certainty. But here's what I can say with confidence: innovation and competition make for a stronger, healthier telecom ecosystem. That's why so many are excited about Open RAN's potential.

And that's why this forum is so timely. We want to encourage research and development into innovative network solutions. One way to do that is by convening the top experts in the field to discuss the benefits of Open RAN, the challenges of implementing it, and the lessons learned from deployments thus far. That's exactly our task today. So I'm grateful our impressive roster of public- and private-sector experts for discussing the current state of Open RAN-related technologies and the path ahead.

Before I relinquish the floor, I want to thank the FCC staff who made this event possible. Among the 31 staffers who brought us from concept to concrete: Ken Baker, Connie Diaz, Kamran Etemad, Monisha Ghosh, Charles Mathias, Robert Pavlak, Wes Platt, Michael Smith, Cecilia Sulhoff, Becky Tangren, Janet Young, and Morasha Younger from our Bureaus; Sean Spivey and Evan Swarztrauber from my office; and, as always, Jeff Riordan and the Commission's AV team.

With that, it's my honor to present this important message from the U.S. Secretary of State, a distinguished Kansan, and my good friend, Mike Pompeo.