REMARKS OF FCC CHAIRMAN AJIT PAI
AT CYFY 2020

OCTOBER 16, 2020

Hello, and greetings from the United States. It's great to be with you.

It has now been eight months since my most recent and probably most memorable visit to India. In February, I was honored and humbled to be a part of the U.S. government delegation visiting India. From my bilateral visits with counterparts in the Indian government to conversations with Prime Minister Modi and the state banquet at Rashtrapati Bhavan, the energy and excitement were incredible. The trip left me with an even deeper appreciation of the common values our countries share and an even stronger determination to help bring the world's oldest and largest democracies even closer together.

Of course, CyFy attracts an international audience. So, greetings to other guests from around the globe.

We are gathering virtually at a pivotal moment in the evolution of communications technology. Across America and around the world, private companies are rolling out the next generation of wireless technology—commonly known as 5G. These networks will bring exponential increases in speed, responsiveness, and capacity—creating an incredible wireless experience for both consumers and enterprises.

At the same time, Wi-Fi 6 is also being introduced. This next generation of Wi-Fi will offer maximum speeds that are up to two-and-a-half times faster than the current standard, along with better performance for connected devices.

Because satellites are smaller and we now have more agile, reusable launch vehicles, we can launch more equipment into space, more safely and more cheaply. These advances have opened the door for companies like SpaceX and OneWeb to begin deploying low Earth Orbit satellite constellations that promise to deliver fast, low-latency broadband services to the hardest-to-reach rural areas on the wrong side of the digital divide in the United States and around the world.

Combine these advances in communications with the processing power of the cloud and breakthroughs in AI and machine learning, and the possibilities are truly staggering. We are moving to a world where everything will be smart and connected. Ericsson projects that an additional 13 billion devices will come online between now and 2024. Some call this future the Internet of Things. Others call it the Fourth Industrial Revolution. I call it transformative.

We are already seeing new and improved services and applications across a series of verticals that will grow our economy and improve our standard of living. Just look at telehealth, where the model of care is being inverted with medical professionals providing services wherever the patient happens to be, as opposed to inside a traditional, brick-and-mortar hospital or clinic. In the U.S., we've seen a huge shift to digital health solutions during the pandemic, and I expect many of these gains to hold.

We've also begun seeing new technologies that can change the lives of people with disabilities. For example, Microsoft has developed an app that uses AI and deep-learning tools to narrate the visual world—describing nearby people or objects with spoken audio for those with visual impairments.

This is all just a small preview of what's to come. 5G and other technologies will certainly unlock many new innovations that we have yet to imagine.

Promoting the development and deployment of 5G has been one of my highest priorities as FCC Chairman. We call our strategy the 5G FAST plan. That plan has three key components: freeing up spectrum, promoting wireless infrastructure, and modernizing regulations to encourage fiber deployment.

This strategy has yielded significant results. For example, we've completed four auctions in less than two years that have repurposed massive amounts of spectrum for 5G. In addition, we continue to modernize regulations and promote infrastructure build-out. This has spurred record-breaking capital investments in infrastructure essential for 5G, including fiber-optic cables and small cells.

But as important as our 5G FAST plan is to facilitating 5G network deployment, these gains can be severely undermined if we can't ensure that these networks are secure.

5G will be embedded in almost every aspect of our economy and society—from businesses to homes, hospitals to transportation networks, manufacturing to the power grid. That means securing our networks will become much more important—and much more difficult.

As the Council on Foreign Relations put it in a recent white paper, "5G networks will expand the number and scale of potential vulnerabilities, increase incentives for malicious actors to exploit those vulnerabilities, and make it difficult to detect malicious cyber activity."

A critical part of network security is 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.

For years, U.S. government officials have expressed concern about the national security threats posed by certain foreign communications equipment and service providers. Hidden "backdoors" to our networks in routers, switches, and other network equipment can allow hostile foreign powers to disseminate viruses and other malware, steal Americans' private data, spy on U.S. companies, and more.

The equipment at the heart of 5G networks currently comes from just a few global suppliers. And the largest right now is the Chinese company Huawei. This has raised concerns, especially because Chinese law requires all companies subject to its jurisdiction to comply with requests from the country's intelligence services, and bars disclosure of these requests to any third parties.

To counter this risk, the FCC has prohibited the use of money from our Universal Service Fund, or USF, to purchase or obtain any equipment or services produced or provided by companies that the Commission determines pose a national security threat to the integrity of communications networks or the communications supply chain. And we specifically designated Huawei and ZTE as companies that pose such a threat.

We also started a process to identify and catalog insecure equipment used in USF-funded communications networks so we can work to implement a program to remove and replace it. We recently completed this review and released our findings earlier this month. We determined that it could cost at least $1.6 billion to remove and replace Huawei and ZTE equipment in U.S. networks that could be eligible for reimbursement under current law. We are working with the U.S. Congress to secure the necessary funding to do just that.

In May 2019, the FCC denied China Mobile's application to enter the U.S. market for national security reasons. Since this decision, we have issued orders to four other Chinese state-owned companies—China Telecom, China Unicom, Pacific Networks, and ComNet—that already hold such FCC authorizations. The orders require these companies to demonstrate why the FCC should not revoke and terminate their authorizations to operate in the United States based on similar national security concerns.

I would note that the China Mobile action reflects our "whole of government" approach to 5G security. This decision was made after a lengthy Executive Branch review of the application and consultation with the U.S. intelligence community, which concluded China Mobile posed substantial national security risks. This is one of many examples of how we are working across the entire U.S. government to tackle the real and documented dangers posed by insecure networks.

And when I say "whole of government," I'm also including the legislative branch. Earlier this year, our Congress passed and the President signed into law the Secure and Trusted Communications Networks Act. This law aims to further strengthen the integrity of communications networks and the communications supply chain, and the FCC has begun implementing it.

These regulatory steps are critical to protect the integrity of our 5G networks. But they are not the only forces at play. Companies building 5G networks have an economic incentive to address security concerns and to find alternatives to untrusted vendors.

Many carriers building- out 5G networks 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. Making the right choices early on in the network planning and deployment process is much easier and ultimately cheaper than trying to correct mistakes once network construction and operation is well underway.

Unfortunately, the lack of vendor diversity in the global 5G equipment market can make it challenging for some carriers to find cost-effective alternatives. The good news is technological innovation has provided a new path to address these concerns.

Traditionally, wireless networks relied on a closed architecture, in which a single vendor supplied the components between the network edge and core. Now, telecom companies have begun developing and deploying open, interoperable, standards-based, virtualized radio access networks. These Open Radio Access Networks, commonly known as Open RANs, offer an alternative to traditional cellular network architecture. And they could enable a diversity in suppliers, better network security, and lower costs.

At the FCC, we are encouraging research and development of innovative network solutions. That's why, just last month, the FCC hosted a meeting of experts from the public and private sectors to discuss the current state of Open RAN-related technologies and the path ahead. One notable participant in this event was U.S. Secretary of State Mike Pompeo. Leadership from our Departments of Commerce and Homeland Security have also expressed support for exploring this technology as a security solution. Several industry leaders, including Reliance Jio President Mathew Oommen, participated in the conversation. A consensus emerged from the forum that Open RAN technologies are already showing great promise in the U.S. and around the world, and that the public and private sectors should continue to collaborate and help encourage their deployment.

As we have pursued our own actions to address security threats, the United States has been working closely with our international partners. Put simply, international cooperation is critical if we are to protect our 5G infrastructure.

There has been substantial recent progress in adoption of policies to secure 5G networks, including the July 2020 announcement by the United Kingdom that it will remove Huawei equipment from its 5G networks. The United Kingdom decision comes as a number of countries across Europe—including the Czech Republic, Poland, Romania, Denmark, Estonia, Latvia, Sweden, and Greece—have taken steps prohibiting these high-risk vendors from their networks. We have also seen telecommunications operators taking actions to make their networks secure. This audience may already be familiar with Jio's actions on this front in India, but Telefonica in Spain, Orange in France, Telstra in Australia, SK and KT in South Korea, NTT in Japan, Orange and Proximus in Belgium, and telecom operators in Canada and Singapore, as well as many others, have made the decision to only use trusted vendors in their 5G deployments.

Efforts to secure 5G networks do not stop at our borders. We are in this together.

On that note of solidarity, thank you for this opportunity to talk about the FCC's approach to these important issues. The United States stands ready and willing to work with all of you to build a brighter digital future.