REMARKS OF FCC CHAIRMAN AJIT PAI
AT THE COUNCIL ON FOREIGN RELATIONS

NEW YORK, NY

NOVEMBER 5, 2019

Last week, I was in Egypt as part of the U.S. delegation to the World Radiocommunication Conference. Today, I'm at the Council on Foreign Relations. And tonight, I'm hoping to see my beloved home-state Kansas Jayhawks play Duke in Madison Square Garden. I'm afraid my decision to be Mike Pompeo for Halloween has gone too far.

It's fair to say that a CFR appearance by the Chairman of the FCC is out of the ordinary. But these are extraordinary times. We're at a pivotal moment in the evolution of communications technology. Across America and around the world, private companies have begun rolling out the next generation of wireless technology—commonly known as 5G.

These networks will bring exponential increases in speed, responsiveness, and capacity. They will enable new and improved services and applications that will grow our economy and improve our standard of living—from connected cars to telemedicine to precision agriculture.

Another way to think about our 5G future is that we are moving to a world where everything will be 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.

The United States is poised to seize these opportunities. At the FCC, we're implementing a plan to Facilitate America's Superiority in 5G Technology. The 5G FAST Plan is already helping ensure that our nation leads the way in 5G deployment. We're making more spectrum available for 5G. We're making it easier for carriers to deploy wireless infrastructure. And we're modernizing our rules to encourage the deployment of fiber to carry wireless traffic once it comes off the airwaves.

But for all the opportunities that 5G will unlock, it will also create new challenges. Chief among these is the main subject of my remarks: network security.

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

A recent Council on Foreign Relations white paper explained well how 5G will change the cybersecurity landscape. It said, "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."

An important 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 providers. Hidden "backdoors" to our networks in routers, switches, and other network equipment can allow hostile foreign powers to inject 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 is a major concern.

Huawei positions itself as a private company. But it has significant ties to the Chinese government, namely, the Communist Party, and China's military. Moreover, Chinese law requires all companies subject to its jurisdiction to comply with requests from the country's intelligence services. These requests cannot be disclosed to any third parties, such as Huawei's customers in China or abroad. That means China could compel Huawei to spy on foreign individuals and businesses and prevent Huawei from disclosing such surveillance requests.

You don't have to look hard to find evidence that the Chinese government is willing and able to use its growing influence over global commerce to advance its own interests. In the past month alone, Chinese officials pressured the National Basketball Association to stamp out criticism from anyone within the NBA of the country's policies in Hong Kong. Gaming company Blizzard Entertainment, which is partially owned by Chinese tech giant Tencent, suspended a professional gamer for speaking out in support of Hong Kong protestors. And Apple, which has extensive business operations in China, removed the Taiwanese flag emoji for iPhone users in Hong Kong and Macau.

These cases reflect a disturbing and growing pattern of behavior by the Chinese government. They also raise a broader concern about the security of the United States. If China is willing to use its leverage over basketball, e-sports, and emojis, imagine what could happen if we let Chinese companies' equipment into tomorrow's 5G wireless networks. This would open the door to surveillance, espionage, and other harms—stakes much higher than sports and entertainment.

For too many years, some have dismissed this concern as hypothetical, or as a smokescreen for protectionism. But if there is a silver lining to the episodes of the past month, it is that millions of Americans have now come to understand that the threats posed by the Chinese Communist Party are comprehensive and all too real.

Even before these latest developments, however, there was no shortage of red flags about Huawei.

Earlier this year, the Justice Department charged Huawei officials with fraud and theft of trade secrets from T-Mobile. The indictment stated that Huawei offered bonuses to employees who succeeded in stealing confidential information from other companies. In announcing the charges, FBI Director Christopher Wray described Huawei's transgressions as "brazen and persistent."

Independent technical experts have similarly raised concerns. A report issued earlier this year by the cybersecurity firm Finite State found that a majority of the Huawei firmware images they analyzed had at least one potential backdoor.

And earlier this year, the United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board issued a damning assessment of the company. It found that a lack of "basic engineering competence and cyber security hygiene" makes Huawei equipment vulnerable to just about anyone, "bringing significantly increased risk to UK operators."

On top of all that, the Chinese government subsidizes Huawei, enabling it to undercut its competitors on price when bidding on contracts, even if the quality is lacking. Whether this violates World Trade Organization rules and other laws I'll leave to the trade lawyers, but this practice demonstrates the Chinese government's strategic determination: choose Huawei as a national champion, make it a key component in its Belt and Road Initiative, and crush foreign competitors by any means necessary.

For our part, when it comes to 5G and America's security, we cannot afford to take a risk and hope for the best. The stakes are too high.

So what can we do to secure our networks?

First, we need to make sure that the equipment going into 5G networks is from trusted vendors—that the companies entering this space won't risk our national security, threaten our economic security, or undermine our values.

This type of upfront solution is just common sense. Making the right choices when deployment is beginning is much easier than trying to correct mistakes once network construction and operation is well underway.

And the good news is that we're seeing a government-wide effort to carry this out.

In 2018, Congress passed a law prohibiting federal agencies from purchasing telecommunications equipment or services that would pose a national security risk, including from Huawei.

In May of this year, the President issued an Executive Order to prohibit the purchase and installation of telecommunications equipment in the United States deemed a security threat. The Department of Commerce was charged with developing regulations, and proposed rules are due to be released soon.

And at the FCC, we're doing our part. In two weeks, the FCC will vote on prohibiting those that receive money from our annual $8.5 billion Universal Service Fund from using it to purchase equipment or services from companies—like Huawei—that pose a threat to the security of our communications networks.

But it's not enough to ensure that risky equipment won't be installed into the networks of the future. That's why we're also working to secure existing networks.

America's largest telecom providers have generally refrained from installing Chinese equipment, but others, particularly some rural wireless carriers, currently have Chinese equipment in their networks. This poses an unacceptable risk. So at our November public meeting, the FCC will also vote on launching a process to remove and replace such equipment from USF-funded communications networks. My plan calls first for an assessment to find out exactly how much equipment from Huawei and another Chinese company, ZTE, is in these networks, followed by financial assistance to help these carriers make the transition to more trusted vendors. We'll seek public input on how big this "rip and replace" program needs to be and how best to finance it. Our goal is to close security gaps in a fiscally responsible way.

The third thing we need to continue to do is to engage with our international partners. We need to remind our allies that decisions impacting 5G security need to be made with the long term in mind. Focusing too heavily on short-term considerations could result in choices that are pennywise but dollar foolish.

The more that we can work together and make security decisions based on shared principles, the safer that our 5G networks will be. When I meet with my foreign counterparts, I stress the importance of 5G security. And I have done that personally and extensively over the past year. Both as part of a cross-Administration team and solely on behalf of the FCC, I've visited and have spoken with senior leadership in Bahrain, Germany, Portugal, Saudi Arabia, Israel, and the United Arab Emirates, and have met with decision-makers from many other countries, such as Brazil, India, Chile and Australia.

And this May, I was honored to be part of the U.S. delegation at a 5G security forum in Prague, where more than 140 representatives from 32 countries came together to build a consensus approach for protecting next-generation networks. We developed a set of recommendations called the "Prague Proposals." This security framework is based on the principles of competition, transparency, and the rule of law.

Having spent the past week meeting with other government officials at the World Radiocommunication Conference in Egypt, I'm encouraged that these principles are gaining traction. There's growing awareness of the importance of supply chain integrity. Indeed, in the last twelve

months, we've seen allies like Japan, Australia, and New Zealand take action to prevent equipment from unsafe vendors into their networks.

Strong international alliances will also be helpful with the standard-setting process for 5G, which is still ongoing. One key focus will be true interoperability, so network operators can stitch together bits and pieces from different vendors. This will keep any one equipment provider from gaining too much market power. At the same time, it would open more opportunities for software providers.

The fourth and final thing that I will highlight this morning is the need to leverage our nation's leadership in software to mitigate security risks. If we can virtualize functions of the radio access network, we can not only reduce the cost of deploying 5G networks but reduce reliance on foreign equipment manufacturers. I am encouraged by the work that American companies are currently doing in this area and hope to see significant breakthroughs soon. As I and my colleagues at sister agencies have made clear to our counterparts in foreign countries, America's current leadership in 5G, and our support of virtualized networks of the future, demonstrate that the choice between 5G development and security is a false one—now and going forward. A country need not choose between the two. And the United States certainly will not do so.

* * *

Ultimately, the Chinese government's increasingly brazen actions to leverage its commercial influence and stifle free expression should be a wake-up call for the United States. They remind us that action is needed—now—to secure America's 5G networks. The FCC and our federal partners are doing just that. And we are on track for a strong and secure 5G future.