KEYNOTE REMARKS OF FCC COMMISSIONER BRENDAN CARR

AT THE INTERNATIONAL INSTITUTE OF COMMUNICATIONS
2019 TELECOMMUNICATIONS AND MEDIA FORUM

"BUILDING A 5G WORLD"

WASHINGTON, D.C.

10 DECEMBER 2019

I would like to thank the International Institute of Communications for inviting me to speak today. As I looked over the program—or, for our international attendees, that's "programme" with an extra "me" at the end—I was struck by the impressive list of speakers and panelists. I think that is a testament not only to the importance of the IIC's mission to provide a forum for balanced and open dialogue in global tech policy, but also to the moment in which we find ourselves.

The growing 5G revolution is a generational upgrade in communications that will fundamentally alter the way in which technology is integrated into our everyday lives. The march of technological improvement will continue to bring the citizens of the world closer together and grow our economies. It is therefore vital that the countries and institutions that we represent continue to work together to overcome our shared challenges and realize our shared goals.

The panels this afternoon will address some very interesting and difficult issues, including data privacy and Artificial Intelligence. But to pull from a theme of some of my recent speeches, I want to be forward looking. Specifically, I want to look ahead to tomorrow afternoon's session on 5G infrastructure.

As everyone here knows, 5G is a disruptive new service that promises 10 times more responsive networks, at 100 times current speeds, that can serve 1,000 times more devices. 5G isn't just an upgraded version of 4G. 5G's performance characteristics and how it is built blur the distinctions between wired and wireless industries. 5G will enable more choice as previously siloed industries compete, which we know will decrease prices and improve quality. And as more 5G networks come online, the already surging demand for data will explode.

Our existing wireless networks cannot handle this coming volume of data. Nor can they perform at the level needed to power the technologies of the future. The fullest vision of IoT sees smart devices scattered throughout Smart Homes, in Smart Cities, and across Smart Ag. 4G networks can't serve that density of devices. The fullest vision of real-time networked experiences—from gaming, to virtual reality, to remote surgery, to autonomous vehicles—requires networks with nearly zero latency. All these life-changing technologies won't work or won't work well without 5G.

Although the benefits of 5G are compelling, the network upgrade won't happen evenly or everywhere unless we get the right regulatory structures in place. After all, many of the largest cities in the U.S.—indeed, the world—might see 5G almost regardless of the regulations we adopt. But that's not success. We want to see next-generation broadband and the economic opportunity it enables available in every community. And smart infrastructure policies are key to doing that—they can flip the business case for thousands of communities.

That's why we've been so focused at the FCC on updating our broadband infrastructure rules. We've done so by modernizing our rules and cutting red tape.

All of these FCC efforts are already delivering results.

Internet speeds are now up 56 percent compared to just two years ago. The digital divide—the percentage of Americans that lack access to high-speed Internet services—narrowed by about 20 percent. Providers built out more miles of high-speed fiber lines last year than ever before. And investment in broadband networks is back on the rise.

The 5G results are especially exciting. America now has the world's leading 5G platform. The very first commercial 5G service launched here in the U.S. more than one year ago. By the end of 2018, the private sector extended 5G to 14 communities. Halfway through this year, that figure expanded to more than 30, and one provider has now committed to building 5G to 99 percent of the U.S. population.

Many of these 5G builds are powered by small cell antennas that provide the fiber-like capacity and millisecond latency that are key for many 5G applications. Because of FCC reforms I mentioned earlier, investment in small cells has boomed. The private sector deployed 13,000 small cells in 2017, and then 60,000 in 2018, and an expected 200,000 total by year's end.

And the benefits of our infrastructure reforms are not just being realized in big cities, but in small communities across the nation. I recently met with broadband builders in Houston's Second Ward, a part of the city that hasn't always shared in the prosperity or investments that its neighboring communities have seen. They were at work trenching fiber and powering up small cells to boost wireless capacity.

Outside of America's biggest cities, we're seeing progress too. Take Sioux Falls, South Dakota. That's where next-gen small cells have been installed that are now live and ready for 5G service.

These figures and examples quantify the momentum America now has for 5G investment. But of course, these next-gen networks must also be secure.

As networks transition from carrying voice calls and emails to these life changing applications, the security of those networks becomes only more important. There's already so much in modern society that now runs on interconnected networks, from banking, to transportation, and even our power grids. This will become only more so as carriers continue to build out 5G networks. If these networks are threatened, everything we have come to rely on is threatened.

In the U.S., we have acknowledged the threat that Chinese telecom firms pose to our networks for some time. In 2012, the House Permanent Select Committee on Intelligence issued a report recommending that companies avoid using Huawei and ZTE equipment. In 2018, Congress passed the National Defense Authorization Act, which prohibits U.S. government agencies and contractors from using Chinese equipment. In May of this year, President Trump issued an Executive Order to secure our ICT infrastructure and supply chains. Separately, the U.S. Department of Commerce added Huawei to the Entity List, which imposes restrictions on its access to U.S. markets, based on a determination that the company engaged in activities that are contrary to U.S. national security interests. And just last month, U.S. Attorney General William P. Barr filed a letter at the FCC stating that "we should not signal that Huawei and ZTE are anything other than a threat to our collective security."

The FCC opened a proceeding on the threats posed by Huawei, ZTE, and other equipment providers last year. The record that developed made clear the security threats posed by these firms. Both companies have close ties to China's Communist government and military apparatus. It's been reported, for instance, that Huawei employees work as agents for the People's Liberation Army. Both companies are subject to Chinese law that obligates them to cooperate with any request from the country's

intelligence services and to keep those requests secret. Indeed, China's National Intelligence Law requires that all "organizations…cooperate with the State intelligence work," and it provides them no right to refuse. It also gives the Chinese government the power to take over a company's communications equipment. Both companies have apparently engaged in conduct like intellectual property theft, bribery, and corruption. And an independent cybersecurity firm recently found that over half of the Huawei firmware images they analyzed had at least one potential backdoor and that each Huawei device they tested had an average of 102 known vulnerabilities.

There is no sign that they will cease these patterns and practices. With this and other evidence, it's not hard to see the threat that companies like Huawei and ZTE pose to our networks and to our national security. And because 5G networks are interconnected, even a small amount of compromised equipment could be devastating to a country's national security. 5G means that we must secure our networks from the "core" to the "edge."

At the FCC, we are in a position to do something about this threat. And we are. Just three weeks ago, my colleagues and I voted to prohibit carriers from using federal dollars to purchase any equipment or services from companies that pose a national security threat, including Huawei and ZTE.

We are not stopping there. In 2018, I called on the FCC to expand our proceeding and put even more options on the table, including the removal of potentially insecure equipment that carriers have already installed in their networks. After all, if equipment poses a threat, it's not enough to stop subsidizing it: it must come out of the network. I am glad that my colleagues joined me in voting in favor of doing just that last week. So the FCC will continue to eradicate the threat posed by insecure equipment in 5G networks.

Importantly, this discussion is not just about network security in some narrow, technical sense. It is also about what I have described as "5G values"—values that China very clearly does not share. Indeed, President Xi Jinping told security officials in January that China does not walk the "Western road" of constitutionalism, separation of powers, or judicial independence. And that's an understatement. Chinese tech companies have a track record longer than a CVS receipt of illegal and malign conduct, which includes violating sanctions, stealing intellectual property, reported lying about extensive partnerships with military and intelligence entities, and enabling extensive and oppressive state surveillance activities.

So part of this conversation—and similar ones taking place across the globe—is about our shared 5G values. We need to work together to ensure that the companies supplying the equipment and services integral to 5G networks are ones we can trust, and are ones that share our commitment to transparency, rule of law, freedom, and individual rights.

I am pleased to report that we are now seeing many countries recognize this position. In March, for instance, the European Commission released a set of recommendations to improve 5G security, which include assessing the risk that equipment vendors could be influenced by third party countries. More recently, in May, the Czech Republic hosted representatives from more than 30 countries to build a common approach to 5G security. That effort produced the Prague Principles, which are a set of recommendations on how to build a secure and trustworthy 5G network. Those principles also recognize the risks posed by a third country wielding influence over an equipment supplier. Australia issued 5G security guidance to protect their networks from unauthorized access or interference by "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law." Japan has imposed requirements to "take appropriate cyber security measures including measures to respond to supply chain risks." Taiwan has extended its existing measures regarding trusted equipment vendors to cover all 5G government networks and critical infrastructure. And most recently, U.S. Vice President Mike Pence and Polish President Andrzej Duda signed a Memorandum of Understanding on 5G security.

So we have seen a great deal of progress on securing 5G networks over the course of the past year. I am confident that this progress will continue and that these next-gen networks will deliver economic opportunity to the citizens we all serve.

Once again, I'd like to thank the IIC for the opportunity to speak with you today, and I look forward to taking your questions.