

**STATEMENT OF
JESSICA ROSENWORCEL
COMMISSIONER
FEDERAL COMMUNICATIONS COMMISSION
BEFORE THE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE
“INDUSTRIES OF THE FUTURE”**

Good morning, Chairman Wicker, Ranking Member Cantwell, and Members of the Committee. Thank you for the opportunity to appear before you today.

I believe the future belongs to the connected. No matter who you are or where you live, you need access to modern communications to have a fair shot at 21st century success. Communications technology is changing at a breakneck pace and this has extraordinary consequences—for individuals, communities, and nations.

In fact, we live in what Thomas Friedman calls the “Age of Acceleration” thanks to the exponential improvements in software, storage, processing, and networking all around us. But if you want an object lesson in just how fast communications technology is changing, consider what life was like at the start of the last decade, just ten years ago. The smartphone revolution was just getting underway. Voice assistants like Siri were still the stuff of science fiction. Humans could reliably beat computers in Jeopardy. And watching what you wanted meant loading a silvery disc into a big, rectangular device. Plus, space technology was out of reach for everyone but the world’s superpowers. Only about one-third of the world was online.

We’ve come a long way. Over the past ten years, we’ve witnessed a 25-fold increase in the amount of digital data on the planet, a 100-fold increase in wireless speeds, and a billion-fold increase in computational power. These developments are like currents that are supercharging our economy and the field of artificial intelligence. They are the forces behind so much that is changing in industries like manufacturing, agriculture, transportation, healthcare and more. And they are not stopping. So we need to harness this energy and plan for this future—and here are three ideas to do just that.

First, we need a plan to deploy 5G technology to everyone, everywhere in the United States. Right now, we don’t have one. As a result, we risk falling behind our global peers in the next generation of wireless leadership.

The stakes are high. With speeds as much as 100 times faster than present networks and much lower latency, these networks will kickstart the next big digital transformation. They will connect more things in more places, fostering all kinds of new economic activity. This in turn, will drive the future of industry and expand the potential for machine learning and the possibilities of artificial intelligence. Connecting the physical world around us will not only change industry, it will change the way we work, and even what work entails.

But to lead in this next generation of connectivity, we need smarter spectrum policy. The truth is we have made a series of choices that have put us behind when it comes to freeing key airwaves we need for 5G. That's because to date the United States has aggressively focused its early efforts to support 5G wireless service by bringing only high-band spectrum to market. We have yet to auction a single megahertz of mid-band spectrum.

This is a mistake. The rest of the world does not have this singular focus on high-band, millimeter wave frequencies. At least sixteen countries have auctioned mid-band spectrum specifically for 5G, starting as far back as two years ago. That means they have a head start on developing a 5G ecosystem in mid-band airwaves.

Meanwhile, our focus on millimeter wave spectrum is threatening to create 5G haves and have-nots in the United States. That's because while these airwaves have substantial capacity, their signals do not travel far. As a result, commercializing them is costly—especially in rural areas. The sheer volume of antenna facilities required to make this service viable will limit deployment to the most populated urban areas. This will deepen the digital divide that already plagues too many rural communities nationwide. That's not right.

But don't take my word for it. Last year the Defense Innovation Board—the United States military's premier advisory board of academic researchers and private sector technologists—surveyed the state of next-generation 5G networks and issued a sober warning. They found that “the country that owns 5G will own innovation and set the standards for the rest of the world” and “that country currently is not likely to be the United States.” Why? As the experts on the board suggested, the Federal Communications Commission (FCC) is prioritizing the early release of high-band airwaves over mid-band airwaves and this is a “fundamentally flawed focus.” I agree.

So the FCC needs to change course, make it a priority to auction mid-band spectrum, and also develop a national plan for 5G service. The bipartisan leadership of four Senate Committees—Intelligence, Homeland Security and Governmental Affairs, Foreign Affairs, and Armed Services—wrote the White House late last year expressing their concern that we don't have a coordinated, national strategy in place for 5G—and we need one. They're right.

As part of this effort, we also need a plan to grow the unlicensed spectrum, or Wi-Fi. Today Wi-Fi contributes hundreds of billions to our economy each year. But going forward we will need Wi-Fi that can keep up with faster 5G speeds—because up to 70 percent of 5G traffic may be offloaded to Wi-Fi. That means the FCC must move faster to secure multiple wide channels for next generation Wi-Fi that will help us realize gigabit-plus speeds in homes, offices, and factories.

Second, we need a plan to invest in training for the jobs of the future. Across the board, we need to do more to prepare our workforce for digital change. We can start with developing the workforce we need to build 5G networks. In the near term, the United States will have to train another 20,000 tower climbers to help install 5G equipment. In the longer term, we will need many other workers for every layer of the 5G ecosystem. But the Department of Labor

currently does not list 5G jobs as a priority for its registered apprenticeship programs. This is a problem—and we should fix it.

At a broader level we need to think about how we can introduce more pathways to upward mobility across industries and across the country. The skills necessary to secure and keep a job are changing fast, but data suggests a steady decline in the amount employers are investing in their workforce. To remedy this, we need to encourage more investment in our workers. It's time to explore a human capital tax credit to offset a portion of new training activities to support the future of work. This could help upgrade our workforce, ensure access to in-demand skills, and create more job security for American workers nationwide.

Third, we need a plan for both device and network security. Our 5G future will feature billions and billions of connected devices in the internet of things. These connections will increase our effectiveness and efficiency. They will inform our choices about how to deploy capital and scarce resources in everything from manufacturing on the factory floor to predicting crop yields on the family farm.

But before we embrace this future, we need to ask hard questions about security. That's because when we multiply the number of things that are connected, we also expand our vulnerabilities to cyberattack. After all, the equipment that connects to our networks can matter as much for security as the equipment that goes into our networks.

So here's what the FCC can do to ensure the internet of things becomes the internet of secure things. Every device that emits radiofrequency at some point passes through the FCC. If you want proof, pull out your smartphone or take a look at the back of any computer or television. You'll see an identification number from the FCC. It's a stamp of approval. It means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States. This routine authorization process takes place behind the scenes. But the FCC needs to revisit this process and explore how it can be used to encourage device manufacturers to build security into new products. To do this, we could build on the National Institute of Standards and Technology draft set of security recommendations for devices in the internet of things. These efforts specify cybersecurity features to include in network-capable devices, whether designed for homes, hospitals, or industrial settings. They cover everything from device identification, device configuration, data protection, access to interfaces, to critical software updates. In other words, they are a great place to start—and we should do it now.

At the same time, we need to focus on the security of our networks themselves. So far our efforts have been limited to improving 5G supply chain security through discouraging the use of insecure Chinese network equipment. But this alone is shortsighted. It's time to expand our approach and improve security by working on unlocking radio access networks through virtualization. This software-centric approach is known as open radio access networks (O-RAN) and it can support a more diverse and more competitive market for secure network equipment. The FCC can help get this started now by building opportunities to test O-RAN in our ongoing effort to authorize city-wide 5G testbeds in New York and Salt Lake City.

Thank you for the opportunity to offer my views on what we need to do to create opportunities for all in the industries of the future. I look forward to answering any questions you may have.