STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *China Mobile International (USA) Inc., Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, ITC-214-20110901-00289

Here's a hard truth: Today no communications system is ever fully secure.

To understand why requires a bit of history. For most of the twentieth century, communications in the United States was synonymous with a single company. That company's monopoly status meant that it controlled all aspects of security for the public switched telephone network. Moreover, communications traffic traveled by and large over buried cable, which provided a degree of physical protection from intrusion.

Then in 1984, courtesy of a court decision, we introduced competition to the communications marketplace. Lower prices and greater innovation followed. But this move also multiplied the number of actors and exponentially increased our security challenges.

The rise of consumer wireless communications came a bit later. Because wireless signals spread as they travel, they are easier to intercept. On top of this, the reliance on cell phone towers made it easy for bad actors to target network providers. Even today, many of these structures have limited physical security.

But the most profound change may be the rise of the Internet. As our lives migrated online, our communications combined control and content into a single channel, vastly simplifying the ability to attack a network and its users. Today the Internet underlies nearly every facet of our lives and is the foundation for much of the critical infrastructure that keeps our country running. But all of this activity is vulnerable to malicious software, denial-of-service attacks, form-jacking, phishing, and a growing range of application vulnerabilities. Billions of people were affected by cyber attacks last year and those numbers are only going to grow.

I started with a hard truth about security and our communications networks—that given the powerful complexity of modern communications, no system is ever fully secure. But that does not excuse us from working to improve the strength and resiliency of our networks. History demonstrates that as our communications capabilities evolve, so do their security risks. It is imperative that we make security a priority and build it into everything we do. So here's another hard truth: The Federal Communications Commission is doing too little to address the vast challenges of network security and safety.

I believe the first duty of the public servant is the public safety—and on that score this agency has work to do.

Please don't get confused by the performative security associated with this decision. This application has been in these halls for more than eight years. It has been on permanent pause. So while I support this vote, it does nothing to change the status quo. Nor does it address any of the fundamental challenges to the security of digital age communications.

To move beyond performative security to real security, this agency needs to change course. This is the right moment to do it. We are at an inflection point as the world races to deploy next-generation wireless networks. With 5G service, we will have wireless capability built into the world around us. This

will provide a whole new range of opportunities for civic and commercial life. But as they multiply, this will vastly expand our surface exposure to attack.

It is no longer enough for the United States to be first to 5G. If we want to ensure our continued technology leadership, the networks we deploy must also be secure. In a speech at the start of this year at the Center for Strategic and International Studies, I offered three ideas about just where the FCC can begin.

First, I suggested that the agency needs to re-charter and reinvigorate the Communications, Security, Reliability, and Interoperability Council and give it a new focus on 5G security. This needs to include more study on security technologies to reduce the risk from the Internet of Things, more study on network function virtualization to reduce denial-of-service attacks, and a new study on supply chain risk management that recommends specific mitigation techniques. Today, a bipartisan group of members from the House of Representatives sent this agency a letter calling for just this approach with the next iteration of this council. I support it and I hope my colleagues will follow my lead.

Second, late last year, the Department of Homeland Security announced the creation of the nation's first Information and Communications Technology Supply Chain Risk Management Task Force. This group is charged with developing national recommendations to identify and manage risk in the global supply chain for communications.

The task force includes officials from the Department of Homeland Security, Department of Defense, Department of Treasury, General Services Administration, Department of Justice, Department of Commerce, Office of the Director of National Intelligence, and the Social Security Administration. In addition, there is expertise from industry, with representatives from communications carriers, equipment manufacturers, and cybersecurity companies.

It's an impressive list, to be sure. But there's one agency that is missing. The FCC needs a prominent seat at this table. Leaving the agency with primary oversight over communications out is neither prudent nor wise. Good things come to those who ask, so it is time for this agency to insist that one of the individuals on this dais to join the leadership of this effort. Moreover, the work of this forum should inform our ongoing proceeding concerning equipment supported by universal service funds.

Third, the FCC needs to make cyber hygiene a priority. To keep our communications systems functioning we are going to need routine practices that increase security and reduce exposure to attack. The agency must build these policies into its day-to-day work. As the number of devices using radiofrequency expands with the Internet of Things, the agency should use its equipment authorization process to encourage device manufacturers to build security into new products. On top of this, the agency could ask that as a condition of holding a public license, licensees certify that they have implemented the best practices for 5G security. This could include a commitment to using the National Institute of Standards of Technology Cybersecurity Framework. While we're at it we need to do more to educate citizens about cyber hygiene. We must increase our outreach with consumers and consumer groups on the basics of cyber hygiene—from downloading software upgrades for devices to assessing connection security when using unlicensed airwaves.

Finally, the honest truth is that we have failed the public when it comes to the privacy and security of wireless devices. Reporting last year and earlier this year indicated that for a few hundred dollars a range of shady middlemen can tell you where any wireless phone is being used within a few hundred meters. Going forward, the potential for abuse is frightening. Remember, new wireless devices will be in our homes—from smart thermostats to virtual assistants to televisions with cameras and microphones. They will be outdoors—from smart electricity grids to adaptive traffic signals. They will

be in our cars, sensing engine operation and location. And they will inform the way we work, shop, seek healthcare, and engage with the world around us. Yet this agency has been silent when it comes to what happened that resulted in location aggregators getting this information from wireless carriers and making it available for purchase. This is an issue of personal and national security. This agency owes it to the American public to explain just what is going on with the privacy of our wireless devices.

Hard truths can make us uncomfortable. But our history shows that if we acknowledge them, they can be a call to action. I think it is time for this agency to act like network security and consumer privacy is a priority. I hope my colleagues are ready to change course and make this happen.