STATEMENT OF
COMMISSIONER BRENDAN CARR

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

The free market is building the next generation of communications networks in America. Broadband providers have invested $1.6 trillion in connecting households to fast Internet. And wireless carriers are spending more than $30 billion per year to upgrade to 5G.

Investors are willing to put that astonishing amount of capital at risk to serve American families because of the open system we have. Our economy is vibrant because people around the globe have confidence that we will uphold the rule of law. We are the top destination for foreign direct investment, attracting $4 trillion—money used to employ our scientists in R&D, our tradesmen in construction, and our farmers in their efforts to feed the world. If you play by the rules here, we welcome your business. That commitment has been at the foundation of our success as a country.

And so in telecom, we don't have nationalized networks. The government's role is to encourage all comers to invest, build, and serve Americans—so long as they play by the rules. The government acts as the referee, not the star player. And in this case, it's imperative that we blow the whistle.

When a company seeks authorization to integrate itself into our communications networks, our security review must consider at least three questions. First, how much control can a foreign actor exert over the company? Second, what evidence do we have about the foreign actor's desire to exercise that control? And, third, if the foreign actor were to act on its malintent, what's the scope of the threat that the specific authorization poses?

Here, the answer to the first question is clear. The People's Republic of China owns China Mobile. The Chinese government controls its management and can direct its actions. Compounding its control by ownership, the Chinese government can compel access to telecom facilities within China on demand. China's 2017 National Intelligence Law mandates that "[a]ll organizations and citizens . . . support, assist, and cooperate with national intelligence efforts in accordance with law." We understand that this vague dictate places Chinese telecoms and their customers under routine and secret surveillance by the People's Republic of China.

Second, we have substantial evidence that the Chinese government intends to surveil persons within our borders, for government security and spying advantage, as well as for intellectual property and a business edge. Just this week, the New York Times reported that hackers working for the Chinese government stole some of our government's most important cybersecurity tools and repurposed them to attack Western allies and businesses. The Chinese reportedly targeted an ally's telecom network, and when the tools were later transferred to North Korea and Russia, those governments crippled British hospitals and shipping companies. They even shut down a Ukranian airport, its postal service, gas stations, and ATMs. There is little doubt that the Chinese government would value additional direct access to our telecom networks for reasons contrary to our security interests.

Third, we must assess the scope of the U.S. authorization at issue. In this case, the Chinese government, through China Mobile, proposes to carry traffic from our shores to international destinations.

The purported business plan is to provide low-cost calls between the U.S. and China. At first blush, this looks like a narrow authorization. Interconnection is not integration, and, in any case, we may assume some security risk whenever traffic goes abroad. This reasoning might be dispositive if interconnection were that simple. But due to least-cost routing, a customer may not be able to choose which company carries the traffic. And once on a particular carrier, the traffic can follow a path of the carrier's choosing. This is what security researchers discovered in November, when Internet traffic originating in Los Angeles and destined for Washington, D.C. was sent on a detour through Hangzhou, China. The Chinese government owns the company that directed the traffic along the puzzling LA-Hangzhou-D.C. route.

So the evidence in this case is clear. After a multi-year inquiry spanning two administrations, the Executive Branch agencies recommended that the FCC deny China Mobile's application due to national security and law enforcement concerns—the first such recommendation, ever. The record here supports that outcome.

In fact, the evidence suggests that we should go even further. The Chinese government owns a number of other carriers that already are operating in the U.S., including China Unicom and China Telecom. Those companies hold the same Section 214 authorizations that China Mobile sought. The evidence I've seen in this case calls those existing authorizations into question. For instance, the decision today cites reports that China Telecom has been hijacking U.S. traffic and redirecting it through China.

So it's time for the U.S. to take additional action. Our national security agencies should examine whether the FCC should revoke those existing Section 214 authorizations, and the FCC should open a proceeding on those matters. Security threats have evolved over the many years since those companies were granted interconnection rights to U.S. networks in the early 2000s. Much if not all of the reasoning behind today's decision appears to apply with equal or greater force to those legacy authorizations. Let's ensure that our decisions from decades past don't inadvertently endanger American interests.

I thank the International Bureau for its work on this item. And I thank Team Telecom for its input. The item has my support.