

**STATEMENT OF GEOFFREY STARKS  
COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION**

**BEFORE THE  
COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION  
UNITED STATES SENATE**

**“OVERSIGHT OF THE FEDERAL COMMUNICATIONS COMMISSION”**

**WASHINGTON, DC**

**JUNE 12, 2019**

Good morning, Chairman Wicker, Ranking Member Cantwell, and Members of the Committee. I’m honored to appear before you as a Federal Communications Commissioner for the first time today and I appreciate the support that I received from all of you to assume this post.

“The future is already here, it’s just not evenly distributed.” Wise words, and ones that excellently frame the state of our digital divide. In this seat, I see a world on the cutting edge of transformational fifth generation of wireless technology, or 5G, that will open the floodgates of innovation – autonomous vehicles, virtual and augmented reality, advanced telehealth, precision agriculture, and artificial intelligence. And I’m excited. But while we press forward with 5G, I am increasingly concerned about the far too many communities that are stuck with “no-G.” There cannot be two Americas – one where those with much get even more, and another for those who are left behind. Researchers have begun to describe the digital divide as “persistent.” I agree. To that end, I see a world in which our “digital divide” is hardening into a state of “internet inequality.” This is an issue that affects not only the US economy, but also the individual dignity of our citizens and our democracy. It is absolutely imperative that we make sure that quality, affordable broadband is available to all Americans.

Where people are connected, great things are possible. I'm particularly excited about how broadband can create healthcare and educational opportunities. For health care, I've seen the power of telehealth while visiting with Corie Nieto, the director of telehealth services at the Nevada Health Center Clinic in Amargosa Valley, Nevada -- population about 1,500. She demonstrated how telehealth technology connects doctors from distant urban centers with patients in rural communities, bringing expertise and specialty services that would otherwise be unavailable to patients in this rural community. For educational opportunities, I recently saw the power of high-quality online education in action when I visited Winston Salem State University (WSSU) in North Carolina. WSSU's program allows students who may not be able to attend traditional in-person classes due to work or family demands, to study at their own pace to acquire skills needed for high-demand jobs. These same students apply what they've learned back home in their communities. For example, Gabriel Bottazzi, a second-career student who graduated from WSSU's online Healthcare Administration program, now runs LliBott Consultorios Médicos, a group of four primary care clinics that focus on serving the Latino community in North Carolina through in-person and telemedicine visits.

The FCC manages billions of dollars of Universal Service program funds intended to ensure that all Americans have the broadband connectivity needed to access programs like those offered by WSSU and the Nevada Health Center Clinic. But to eliminate internet inequality we must understand the scope and scale of the problem. The fundamental question is this: does the FCC truly know who has broadband and who does not? Unfortunately, at present, it appears that we do not, and the problem begins with the data. The FCC's recently-released broadband deployment report is, unfortunately, a glaring demonstration of our shortcomings. The first draft of the 706 Report was based on data that overstated high speed broadband connections by more

than 62 million connections – that’s more than the populations of Mississippi, Washington, Texas, Michigan, and Illinois put together. This is troubling for a host of reasons: that the FCC’s data practices lack the sophistication to catch such a significant error by a new entrant; that we had to rely on an outside party to catch the mistake; that a draft with an error of this magnitude was circulated for consideration; that the inaccurate numbers from the draft were publicized in a way that overstated our progress on addressing access disparities; that it took months to correct the data; and that the fluctuating data did not change the FCC majority’s analysis in any way. And, even when our data is reported correctly, it still doesn’t paint an accurate picture in many instances. Under the current system, if a provider reports that it does, or even could, connect a single home in a census block, we count the entire census block as if everybody who lives there is connected. It’s no secret that the FCC’s broadband maps have problems. It’s past time that we fix this.

Right now, the FCC is considering imposing an arbitrary budget cap on all USF programs. But instead of imposing an arbitrary cap, the FCC should get the data needed to produce granular and accurate maps of where broadband is and is not available in the U.S. The status quo is not good enough – not by a long shot. In short, the FCC should be focused on mapping not capping.

I’d also like mention a universally hated phenomenon – robocalls. Robocalls have overwhelmed the network and consumers, and have fundamentally changed the fabric of our culture – we don’t pick up our phones anymore. These calls range from annoying and disruptive to deceptive and dangerous, defrauding unwitting consumers out of real money. Often, calls are spoofed to appear like they are coming from a local business or neighbor. This pernicious practice makes it impossible to differentiate these unwanted robocalls from calls coming from

our pastor, doctor, or kids' schools. Put simply, by allowing these calls to proliferate, we've broken phone service in this country.

I supported the Commission's action last week to clarify that voice service providers can offer call blocking service by default on an opt-out basis. This action should make these tools available to millions more consumers. And the FCC spoke clearly – we fully expect these services to be offered to consumers for free. Free. Because if not, the FCC will know about it, and initiate a rulemaking to prohibit these charges.

We live in a nation that runs on networks. The importance of fixed and wireless communications to the U.S. economy can't be overstated. They are critical to military and government communications, utility infrastructure, every sector of business, and the billions of personal emails, phone calls, and text messages sent in America every single day. Looking forward, as the Internet of Things emerges and billions of cars, appliances, and other devices come online, the importance of our networks will only grow. Network Security is National Security, and right now there are threats in our communications networks – national security threats posed by unsecure Chinese telecommunications equipment with vulnerabilities that carry the risk of espionage or surveillance, and the ability of foreign entities to cripple our communications networks in times of a national emergency. These threats are serious and their presence in our networks is a problem. And while the President's recent Executive Order barred U.S. companies from buying or using telecommunications equipment deemed to be a national security risk moving forward, it did not address the fact that our networks already contain and depend on much of this equipment.

I have said that we need to “find it, fix it, and fund it.” The FCC needs to step up, using its own authority and working with other federal agencies, to investigate and determine the scope

of our network's exposure to these threats. We must **find** any equipment that poses a national security threat. We must **fix** it to secure our networks. And we must **fund** the transition of carriers away from insecure equipment in their networks as rapidly as possible. This may require "ripping and replacing," but it must be done in a way that minimizes disruption to carriers and their customers. This is a national problem that needs a national solution. It could be expensive—estimates range from \$150 million for mitigation measures to over \$1 billion for full replacement as we offset the cost of purchasing and installing new, secure equipment. But our national security is at stake and we must act to protect it.

Finally, I want to reiterate my call for the Commission to act in response to wireless providers selling customer location data. With each passing month, our inaction becomes harder to explain and more problematic. This outrageous practice allowed anyone with a few hundred dollars to purchase anyone else's real time location. As a former federal prosecutor, I've personally petitioned courts for restraining orders to protect survivors of domestic abuse. And I'm shocked to think that an abuser could illegally track a survivor's phone to a safehouse or a shelter. The misuse of this data is downright dangerous. This practice was first widely reported more than a year ago, yet the Commission still hasn't acted against those responsible. The passage of this much time is significant - the Commission typically has only a year to act before statutes of limitations run out. We need to act now.

In closing, I am honored to serve the American people. We have a lot to do, and I look forward to working with my colleagues to address the many challenges ahead. Thank you for the opportunity to testify today. I look forward to answering your questions.