Statement of
Commissioner Geoffrey Starks at the
Center for American and International Law
Institute for Law and Technology

December 4, 2019

Thank you very much for having me today. As I look down the schedule for this conference, I see a list of some of the most interesting—and challenging—issues we face at the intersection of technology and the law. I appreciate the opportunity to kick off these discussions with some thoughts about the 5G era and the communications networks that support many of the technologies you will be thinking about for the next two days.

As communications networks have become more ubiquitous, and more deeply imbedded in every aspect of our society, old silos are breaking down. We can no longer think of our country's economic success, our security, and our geo-political relations as distinct issues. The networks that intertwine people tie these issues together, and I'm encouraged that we're increasingly thinking about them holistically. With that theme in mind, I want to highlight three areas where we're still working to make our policies fit the 5G era: communications infrastructure, security, and democratic engagement. Our prosperity in the coming decades will depend on how well we work to get all Americans connected, ensure the security of those connections, and use technology to protect our democratic values. Today, I want to talk about what we need to do to make that vision a reality.

First, we must work to connect all Americans to modern communications infrastructure. Here in North Texas, surrounded by some of the world's largest tech companies, it can be easy to forget that even basic internet access hasn't reached all Americans. Nearly two million households in Texas don't have access to high-speed internet service. According to the National Digital Inclusion Alliance, Laredo and Brownsville are two of the worst connected cities in the United States. Texas isn't alone in this problem, and there are communities across the country that remain unconnected. This is a stark reality. Broadband is the basic tool of our digital world—something everyone needs to get job, do their homework, pay their bills, and accomplish every other online task many of us take for granted—and we haven't finished the work of getting access to all Americans.

It has been 25 years since the phrase "digital divide" was first introduced. Clearly, then, we are not talking about a temporary condition. Internet inequality is a persistent problem that is only growing in urgency. Low-income people, people of color, and people in rural areas either aren't getting online or are making great sacrifices in order to get connected. For example, according to a Pew Research study, only 45 percent of adults with incomes under $30,000 have broadband at home. That means driving to the library to fill out job applications and joining the waitlist for a Wi-Fi hotspot. There is a striking loss of dignity that manifests when an individual has to work a lot harder for a critical necessity that others take for granted. It's also taking a toll on our economy. A report by the U.S. Chamber of Commerce and Amazon estimates that better online tools and technology

would have allowed rural small businesses to create an additional more than 300,000 jobs with $13 billion in wages per year.

Since joining the FCC nearly a year ago, I have traveled around the country to see this problem up close. In August, as part of a visit to Tribal Lands in New Mexico, I visited the Pueblos of San Felipe and Santo Domingo, New Mexico. We heard from community leaders and members of the Middle Rio Grande Valley Tribal Consortium about their quest to bring futureproof fiber connectivity to libraries in communities where many don't have home broadband service. Cynthia Aguilar, a librarian with the Santo Domingo Pueblo Library, compared the impact of broadband connectivity to the arrival of the railroad to the Pueblo a century ago.

The lengths these communities go to bring affordable service to their citizens inspire me to keep working toward solutions for internet inequality. Solving this problem is a moral imperative. But it is also essential to our global competitiveness going forward. Other countries are making enormous investments to get their citizens connected to high-speed, quality broadband. China, for example, plans to deploy fiber-optic connections to 80 percent of the homes in that country. If we leave so many millions of our fellow Americans behind, our country will fall behind.

That's why I have formulated a four-point plan to make FCC support for expanding rural broadband more effective: 1) funding rural broadband with fixed maps; 2) advancing more affordable internet connections; 3) incentivizing future-proof connections; and 4) investing in responsible auction winners.

On the first point, the FCC must ensure that our spending is driven by good data. For decades, the Commission has worked to address the digital divide. Yet, throughout that period, we've based our funding decisions on mapping data that doesn't reflect the reality of where there is broadband service and where it isn't. Most recently, the FCC proposed $20.4 billion dollars for the 10-year Rural Digital Opportunity Fund. As a native Kansan, I fully support providing the resources needed to adequately address connectivity in rural communities. But I have serious concerns about how the FCC plans to administer this program. Congress, rural underserved communities, and industry experts have repeatedly admonished the FCC to fix its data and maps.

The Commission currently proposes to spend $16 of the $20 billion dollars—nearly three-quarters of the USF support the FCC intends to use over the next 10 years—before it has fixed the data and maps that nearly every stakeholder agrees are badly flawed. I agree with the desire to get support where it's most needed, and believe that the Commission should have chosen to proceed with a smaller initial budget and a shorter service term while we fix our maps. Once we have improved data and maps, the Commission could then proceed with the bulk of the additional support for longer terms. Unfortunately, the Rural Digital Opportunity Fund structure adopts a "ready, fire, aim" approach that favors speed of funding over results.

Second, affordability. As we work to bring the benefits of the 5G era to all communities, we must also keep cost in mind. All the access in the world isn't meaningful to Americans who cannot afford the service. Last week, Tim-Berners-Lee, one of the founders of the World Wide Web, called for a "radical intervention" to make sure the web

"lives up to its potential." Among many other things, his plan calls on governments and companies to make internet access affordable so that no one is excluded. I'm eager to hear from stakeholders—including you all—about how the FCC can do better on this front.

As a next step, when I testify before Congress tomorrow, I will propose that we require rural broadband auction winners—those companies that win licenses to use our universal service subsidies at auction—to offer an affordable broadband service option. The average family spends $2,700 per year on their internet, phone, and cable service. For many working families dealing with increasing expenses and nearly flat incomes, that's just too much. Currently, we know that a number of ISPs, including Comcast, Cox, AT&T and Spectrum, among others, provide low- cost internet offerings around $15 or less to families participating in federal school lunch and other programs – a good start for us to examine what an affordable offering may look like. All Americans should have access to broadband that they can afford. Nobody should be overlooked in our increasingly networked society.

Third, we must incentivize providers to bring future-proof broadband to our communities. As recently as five years ago, some communities received Connect America Fund I (CAF I) funding for service that is so slow that these communities are now counted as unserved today! Those communities are now eligible for additional funds under the 10-year Rural Digital Opportunity Fund—another round of federal funding—to get them up to actual broadband speeds. This experience crystallized for me that we must better understand how our rural telecom support programs have performed historically so that we can better tailor the performance of rural broadband programs for the next 10 years. That's why I've called for the FCC to conduct a data-driven 10-year look-back on how our program has effectively performed in bringing broadband to our unserved areas. The Commission has a responsibility to ensure that its policies are working, and the USF program is an important example of where we can do better. We must understand how our rural telecom support programs have performed so that we can better tailor the performance of the RDOF for the next 10 years. Sometimes you have to look back to move forward. Where have we succeeded? Where did we miss the mark? Which communities have had their connectivity needs met in the way that we expected? Which haven't, and why? Above all else, we must avoid waking up 10 years from now—having spent another $20 billion—still failing to understand which communities are served, and which are not.

Finally, responsibility. As we sit here, unfortunately, more than a dozen CAF-II auction winners have already defaulted on their bids to provide service to rural areas in states like Arkansas, Minnesota, Michigan, Nevada, Nebraska, Colorado, Missouri, Oklahoma, Kansas, Massachusetts, and Virginia. We need these providers to provide service to the hardest to meet residents. Before we send an additional $20 billion dollars out the door, we need to be absolutely sure that all carriers who receive funding are stable and designed to meet our buildout requirements to deliver connectivity to communities that are in need.

Here's the takeaway: connecting all of our citizens matters to more than just those Americans who remain unserved. Our shared economic goals, our security imperatives and our standing in the international order are also very much intertwined in getting all Americans connected to our modern, digital world.

That brings me to the second priority I want to talk about today: we must take steps to ensure that our economic interconnectedness makes us more, not less, secure. Network security is national security. With the growth of 5G wireless services, we are rapidly moving into a world where billions of IoT devices will operate our critical infrastructure, health care systems, financial sector, and transportation systems. Secure networks therefore are not only necessary to preserve the confidentiality and integrity of our communications, but also to protect our public safety.

This is a central concern for me because Congress established the FCC to promote the safety of life and property and for the national defense. With that mission in mind, over the last few months I have laid out my vision for what needs to be done to address network security concerns in the U.S. in addition to the work underway by other parts of the government. The bottom line for me is that I think that we need to address, in a serious way, security problems that are present in our networks now and develop of forward-thinking approach that spots threats before they become a problem.

One issue we're currently tackling is the presence of untrustworthy Chinese equipment in our networks. You've probably heard elected officials talk about "winning the race to 5G." China is laser-focused on that race, too, and is working aggressively to achieve dominance in 5G standard setting and network deployment. China has used many tools to pursue that goal, including defeating market-based competitors by using Chinese manufacturers like Huawei and ZTE as industrial policy instruments in its efforts to achieve 5G dominance around the globe. China's actions certainly raise questions about the potential for that country to use future 5G networks constructed by Chinese manufacturers for espionage or cyber-attacks – questions that we must resolve to strengthen our security. I was proud to join my colleagues last month in voting to prohibit the use of universal service funds for the purchase of equipment from certain Chinese telecommunications companies and to investigate what to do about the equipment already in our networks.

Looking ahead, there is much more to do. Many of the carriers with untrustworthy Chinese equipment already in their networks are small and rural operators working with small teams and tight budgets. They now understand the significant risks their networks face and want to get them fixed. But they're going to need help, and the FCC needs to move quickly to get those systems in place.

I have similar concerns about the parts of the network we rarely think about in our daily lives. Most conversations about the 5G era rightly focus on mobile devices and the coming explosion of data traffic. Cisco predicts that global mobile data traffic will increase sevenfold between 2017 and 2022. All that data that begins wirelessly eventually finds its ways to wired networks and gets passed around the world across a network of undersea cables.

These cables literally link us to other nations, and the FCC is the agency directly responsible for approving them, which means considering and ensuring that these links support our national security. Right now, there is a developing issue involving the plan to construct an undersea cable between Los Angeles and Hong Kong. This project, which is backed by major U.S. companies and China's fourth-largest telecom provider, could end up carrying a large portion of the communications between the U.S. and Asia. The Justice Department is worried that communications over the cable could be stolen, blocked, or

modified on its Hong Kong end, and is consulting with other agencies about their recommendation to the FCC. Ultimately, it is up to the FCC to approve or deny the cable, or to condition its approval on certain mitigations. In the past, we have conditioned our approval on things like mandatory site visits, financial audits, cybersecurity, and network security plans. For my part, I'll decide my position once I have assessed the full record to determine whether any proposed outcome protects the national defense and the safety of life and property—which is the FCC's statutory direction in this area.

Going forward, I am focused on several steps we can take to secure our networks for the 5G era. First, I think we should make sure that American carriers are actually taking advantage of the new security features the 5G standard has to offer. One of the most important is virtualization. Much of the network core and edge processing functionality in a wireless network today takes place on physical hardware. 5G will allow operators to move many of those functions into the virtual world—make it more flexible, customizable and programmable. I think of it like antibodies in the human body that can go wherever, whenever they're needed. When a new type of attack is discovered, the operator can immediately deploy a security element like a firewall to the exact spot under attack. And it can be automated, so it can happen instantaneously, rather than waiting for a human being to identify the problem and deploy a solution.

I think this is an important tool in the network security toolbox. That being said, I understand that many network operators are still learning how virtualization works. According to a report from AT&T's cybersecurity group published last week, less than one-third of network operators surveyed plan to implement security virtualization in the next two years. Network operators in the United States must be incentivized to deploy the most modern security tools available.

We must also seize the opportunity to encourage the growth of American technology. We cannot entrust addressing the technological solutions to the challenges of 5G to our geopolitical rivals. American ingenuity has historically dominated the research, development, and deployment of telecommunications technology. This must continue for 5G, and American companies are already developing alternatives to traditional telecom equipment infrastructure through software-enabled 5G and virtualized radio access networks for cloud-based 5G. 5G infrastructure development must represent the next frontier of American technological leadership.

American 5G equipment will be safer because we can be confident about it observing best practices and protecting our intellectual property and privacy from foreign actors. Most importantly, American companies do not answer to the directives of adversary states with no clear rule of law. Moreover, while artificially low prices may have provided a temporary advantage to Huawei and ZTE, I believe that the telecom industry has come to realize that the cost and inconvenience of fixing and replacing untrustworthy equipment far outweighs any short-term savings. I believe America can rise to the challenge and ultimately come out of this situation more advanced, more secure, and more prosperous.

Finally, all of the investments I have just described are at risk if we don't take steps to protect our democracy and democratic values. Some of the risks to democracy are quite direct. For example, in just a few months, Americans will begin the process of choosing the presidential nominees. Through our intelligence agencies, we know that

foreign adversaries will once again seek to interfere with our elections. Though securing our voting equipment has been a topic of national conversation in recent years—we have heard a lot about maintaining paper ballots and audit trails—I am convinced that we haven't done enough to address the ways our voting equipment is connecting to the network.

Reliance on a wireless network connection, through a cellular connection, Wi-Fi, or other technology, increases a voting system's risk of security failure or vulnerability, and it increases the attack surface that foreign adversaries can target. Remote, wireless access to voting equipment could potentially allow attackers to view or modify all the files in a voting system—including election results and ballot records. That's why experts at the National Institute of Science and Technology and the Election Assistance Commission recommend that networking features in voting machines be disabled by default.

Despite these warnings, some states—including Florida, Illinois, Michigan, Maryland, Rhode Island, Wisconsin and Washington, D.C.—use voting machines that are capable of transmitting results on the ordinary wireless networks we use for our mobile phones. That means those devices are subject to the same threats as other wireless communications. Voting results can be blocked or altered by criminals or adversary states using fake cell towers or by hacking untrustworthy or insecure routers. Because of these risks, I've reached out to the major wireless carriers to discuss how they're protecting their network security and working with election officials. I was pleased to learn that AT&T is working with the state of Texas to improve election-related cybersecurity, and I look forward to working with experts across the telecommunications sector to secure this very important aspect of our networks. The ultimate goal is clear: make sure that every vote, wherever made, is counted accurately each and every time.

Securing our elections is critical and urgent, but it shouldn't be the end of our efforts to make sure democratic values lead in the 5G era of ubiquitous connectivity. More and more, we hear about China pushing ahead on technologies like artificial intelligence and facial recognition technologies. There is a perverse logic behind those advances: it's easier to develop widespread facial recognition, for example, in a country whose laws don't prioritize civil liberties or individuals' privacy. Discussions like the ones you are having this afternoon are an essential part of ensuring that those technologies develop in way that is consistent with our values.

* * * * *

In closing, though I have outlined a number of big challenges that demand our focus, I want to emphasize that I am optimistic about American leadership in the 5G era. We have an enormous opportunity before us to advance American technologies in ways that are consistent with our values. The Internet of Things, smart electrical grids, and autonomous vehicles all raise the stakes, but American innovation is hard at work on those problems. And right now there is an emerging bipartisan consensus that we cannot outsource the technological solutions to geopolitical rivals. If we work together, I am confident we can build a future that is more advanced, more secure, and more prosperous. Thank you again for having me today.