REMARKS OF
COMMISSIONER GEOFFREY STARKS
BEFORE THE
2021 WINNIK FORUM
WASHINGTON, DC

NOVEMBER 18, 2021

Thank you, Ari, for that introduction and for inviting me to join you in honoring Joel Winnik's legacy. Again this year, you have assembled a fantastic group of experts on some of the most pressing issues facing the technology and telecom sectors. What a wonderful tribute! I know you've just finished a panel discussion on emerging trends in consumer protection, and I want to focus on how we can create a consumer-centered modern communications sector.

Before I outline some of my consumer protection priorities, I want to underscore why these consumer protection issues are so important. If you're joining today's event, there's a good chance you have heard me talk about the digital divide before. And you probably know that we have a lot of work to do in the United States to make sure everyone shares the benefits of the digital age. So I'll skip the history and cut straight to today: COVID-19 has taught us that the digital divide isn't just unfair and cruel—it's a threat to our public health and economic security.

And like so many other aspects of the pandemic, the lack of access to and adoption of home broadband has amplified and reinforced existing inequities in our society. Today, Americans of color remain, by a wide margin, less likely to have a home broadband connection than their counterparts. The Pew Research Center has found that 29 percent of Black adults and 35 percent of Latinx adults do not have a home broadband connection. And it's not just those in rural areas who lack access to broadband. In fact, three times as many households in urban areas remain unconnected as in rural areas.

Bridging those gaps will require the historic investments in infrastructure the federal government is now poised to deploy—a hot topic this week. The tens of billions of dollars in fiber and other broadband infrastructure, along with many programmatic upgrades, are absolutely essential to closing the digital divide. But we must meet the disconnected where they are. In that way, broadband needs to be the kind of service—affordable, fair, secure, and private—that Americans want to invite into their homes. From where I sit, consumer protection in the broadband market is an adoption issue and must be part of our national strategy to get everyone online.

First, affordability. All the advanced infrastructure in the world won't help if ordinary people cannot afford to buy the broadband service it supports. For tens of millions of Americans, the price is just too high. A new study by Education Superhighway found that 18.1 million households, home to 47 million people, remain offline because they cannot afford any of the available internet connections. And millions more have made difficult sacrifices to keep the broadband on. No family should have to choose between keeping the lights on and a broadband connection, but we know that they do.

COVID-19 put these challenges into sharp relief. This spring, the New York Times highlighted the challenges facing Jordyn Coleman, a fifth-grade student in Clarksdale, Mississippi. Jordyn, who transferred schools during the pandemic, described his struggles with online school. Jordyn's family does not have internet access at home, and he can only participate in virtual classes by using his mother's cellphone. But his mother works night shifts as a security guard at a casino and, like most of us, takes her phone with her. Ms. Coleman has difficulty making it home in time for Jordyn's first morning classes due to her 40-mile commute on public transportation. Consistently connecting to online lessons would no doubt be easier with a home Wi-Fi connection. But for a family that has faced stiff economic headwinds during the pandemic, other basic needs have to come first. Ms. Coleman usually makes dinner on a hot plate or in an electric pot because she does not have a refrigerator or stove in her apartment. She told the Times: "My priorities are a stove, a fridge, a car. . . . Then maybe we can talk about internet."

Millions of Americans face these difficult choices, and Congress responded with a $3.2 billion emergency investment in affordability. Through the Emergency Broadband Benefit, we're giving lower-income families a $50 or $75 credit on their broadband bills. More than 7 million households have signed up so far. Hundreds of organizations have partnered with FCC to get the word out about EBB, and we're grateful for all their hard work.

At the same time, we have tens of millions more eligible families to reach. Earlier this week, President Biden signed legislation that will convert EBB into a long-term program with $14.2 billion in additional funding. That change should give more providers and more eligible households confidence that this program will work well for them—and not just for the short term. At the Commission, we're working hard to get that new effort, the Affordable Connectivity Program, ready to go by the end of this year. I expect we'll be putting out a public notice soon, and I look forward to your comments.

Support for low-income families is, of course, only part of the solution. We all know that more competition pushes prices down. There will be plenty to say over the coming months about how we can ensure that our historic infrastructure investments lead to more choice. Today, I want to highlight one part of the path forward that I expect to kick off at the Commission soon: As part of the infrastructure package, Congress has specifically directed us to focus on improving price transparency. That means we will soon be collecting and publishing price information from broadband providers participating in the Affordable Connectivity Program. We were also directed to adopt rules to require broadband providers to provide a "nutrition label" that displays prices and other service details in an easily digestible format. This will make it easier for consumer to shop around for the best price and service terms. Stay tuned.

Second, fairness. Ensuring that communications companies treat their customers fairly is one of the FCC's most important jobs. But when it comes to broadband, the Commission has not stood tall on that responsibility in recent years. When past Commission leadership reversed the Open Internet Order, they didn't just eliminate rules banning blocking, throttling, and paid prioritization—they abandoned virtually all of the Commission's regulatory oversight over broadband providers. We are still working our way through a worldwide health crisis in which

the internet has proven essential to keeping our economy running and our citizens connected. The Commission needs to reclaim its authority to protect vulnerable consumers and ensure a vibrant, competitive broadband marketplace.

Third, security. The bigger our reliance on technology, the more we have to lose from security threats. Over the past decade, our networks have faced a rising tide of activity by adversary states and others intent on compromising Americans' privacy and security. That reality came home for millions of Americans this spring when a ransomware attack on Colonial Pipeline, which controls nearly half the gasoline, jet fuel, and diesel on the East Coast of the United States, caused fuel shortages across the southeastern part of the country. Last year, in the midst of enormous strains on our healthcare system, a cyberattack forced one of our largest hospital systems to return to pen-and-paper charting when its network went down.

With those threats in mind—and recognizing that these are whole-of-government issues— much of my time at the Federal Communications Commission has been spent working to secure U.S. networks against potential bad actors. Congress explicitly created our agency "for the purpose of the national defense" and "for promoting safety of life and property through the use of wire and radio communications." The complexity of protecting the American public and the fundamental inter-connectedness of security issues, along with long-term economic and international trends, including the disappearance of the American telecom hardware sector and the growing role of Chinese vendors, have compelled the FCC to embrace that role. Network security is national security.

During the last few years, both Congress and the Commission have focused on getting untrustworthy equipment out of our country's networks. Last month, the Commission began accepting applications for $1.9 billion in funding for reasonable expenses incurred in removing, replacing, and disposing of Huawei and ZTE communications equipment and services. Consistent with the Secure Equipment Act, signed by President Biden last week, the Commission will also establish rules stating that it will no longer review or approve any authorization application for equipment that is on the list of covered communications equipment or services.

Although the Commission's efforts to promote supply chain security have focused on network infrastructure, our networks also include billions of end user devices. As the Internet of Things flourishes and connects a variety of devices to our networks, we must ensure that those devices and the Americans who use them are protected from cyber-threats. According to one study, we will have more than 25 billion connected devices worldwide by 2025. Networks of IoT devices will help our environment by reducing carbon emissions and waste, increase productivity, protect public safety, and generally enhance our way of life.

But many of these devices or their components come with exploitable security vulnerabilities. This same inexpensive equipment is most likely to be used by small businesses and consumers. One 2017 study reported that nearly half of all companies that use IoT devices have lost revenue due to a security breach, at a cost of more than 13 percent of revenue for companies with annual revenues under $5 million. Each device could be a potential entry point for a hostile actor to attack connecting networks. Late last year, for example, a technology news

site found suspicious backdoors in affordable Chinese-made internet routers and Wi-Fi extenders sold at several major retailers that would allow an attacker to remotely control not only the devices, but also any devices connected to the same network. Further testing showed that these backdoors were not only potential threats, but that third parties were actively attempting to exploit them. The Commission should work with other policymakers and retailers to ensure that all devices imported into the United States and connected to our networks meet NIST cybersecurity standards. We also must develop proactive safeguards to educate users and prevent future intrusions on our IoT networks.

Finally, privacy. We need a similar commitment to protecting consumers' privacy online. Americans have good reason to be skeptical. Practically every day, we learn about new data harms: algorithmic and facial recognition bias; companies failing to protect our most sensitive information from hackers and thieves; and "pay to track" schemes that sell location information to third parties. These practices are especially insidious because they replicate and deepen existing inequalities in our society.

For example, millions of Americans saw the New York Times reporting in December 2019 that illustrated, sometimes in frightening detail, how much can be learned about a person from the location of their smartphone. Using supposedly anonymous location data, the Times was able to follow the movements of identifiable Americans, from a visitor to Central Park to then-President Trump himself.

This issue, like network security, requires a whole-of-government response. But I fundamentally disagree with those who say the FCC should sit on its hands. For years, we have known that communications companies can and do access enormous stores of highly sensitive customer data. As many of you know, last year the FCC adopted an enforcement action against the four major wireless carriers for misusing customer location data in violation of the FCC's rules on Customer Proprietary Network Information, or CPNI. Among other problems, those cases highlighted the need to carefully supervise and limit the third parties who get access to sensitive customer data.

More recently, the Federal Trade Commission unanimously approved the issuance of a new report on internet service provider privacy practices that details what the FTC describes as "troubling data collection practices among several of the ISPs, including that they combine data across product lines; combine personal, app usage, and web browsing data to target ads; place consumers into sensitive categories such as by race and sexual orientation; and share real-time location data with third-parties."

That report is a wake-up call. I know that there are jurisdictional and legal issues to be resolved. To fully address these harms, we need to close the gaping holes in our oversight over broadband providers that I mentioned earlier. But the FCC should not shy away from that debate.

While we are doing that work, we should not overlook existing sources of authority. We need to vigorously enforce our CPNI rules and build on the bipartisan agreement behind the 2020 location data enforcement actions. And we should consider how we can use our authority

over the USF programs to protect newly connected people. Here's one alarming example: earlier this year, there were several credible media reports that the phones being distributed to Lifeline beneficiaries came with pre-installed Chinese malware. This malware opened backdoors to outside, undetectable monitoring and interference. In at least one case, the malware was impossible to remove. These kinds of abuses should be alarming to all of us. We shouldn't ask low-income people to trade their privacy and security for these benefits, and we shouldn't let these kinds of stories deter people from taking advantage of an important benefit.

* * * * *

This is, to be sure, an ambitious project. Creating a consumer-centered broadband market where high-quality service is affordable, fair, secure, and private is a big job. It's worth it. Thank for your time, and I look forward to answering your questions and working with you on these important issues.