



MEMORANDUM

September 24, 2019

To: Subcommittee on Communications and Technology Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on “Legislating to Secure America’s Wireless Future”

On **Friday, September 27, 2019, at 9:30 a.m. in the John D. Dingell Room, 2123 of the Rayburn House Office Building**, the Subcommittee on Communications and Technology will hold a hearing entitled, “Legislating to Secure America’s Wireless Future.”

I. KEY FCC SPECTRUM ISSUES AND PROCEEDINGS

Electromagnetic spectrum—often referred to only as spectrum—is used to deliver radio, broadcast television (TV), cellular, and wireless broadband internet services, including 5G wireless technology. There is a finite amount of spectrum available. The Federal Communications Commission (FCC) manages the commercial use of spectrum¹ while the National Telecommunications and Information Administration (NTIA) manages federal use.²

Wireless service providers are seeking a range of spectrum bands (low, mid, and high) to deploy 5G services.³ Some others would like for that spectrum to be reserved for unlicensed use or made available for shared use.⁴

Depending on the frequency, spectrum has different characteristics. High-band spectrum fades over shorter distances and is less able to penetrate buildings and trees than mid- or low-band spectrum, which can travel over greater distances without being deflected by obstacles.

¹ Communications Act of 1934, Pub. L. 104–104, title I, § 104, Feb. 8, 1996 (codified at 47 USC § 151 *et seq.*)

² National Telecommunications and Information Administration Organization Act, PL 102–538, Oct. 27, 1992, *as amended by* PL 115–141, Mar. 23, 2018 (codified at 47 USC § 901 *et seq.*)

³ Federal Communications Commission, *The FCC’s 5G Fast Plan* (<https://www.fcc.gov/5G>) (accessed July 11, 2019).

⁴ *See, e.g.*, John Eggerton, *Microsoft Petitions FCC for White Spaces Rulemaking*, Multichannel.com (May 3, 2019) (www.multichannel.com/news/microsoft-petitions-fcc-for-white-spaces-rulemaking).

The existing contiguous blocks of low- and mid-band spectrum available for commercial use will not necessarily be able to keep up with the growing demand for data.⁵

A. Licensed Spectrum

Recently, the FCC has taken a series of actions to make more mid- and high-band spectrum available for licensed 5G wireless broadband services. In July the Commission adopted an order that made the 2.5 GHz band, which had previously been reserved for educational entities, available to commercial entities and also established a priority filing window for rural Tribal Nations, to be followed by a public auction of any remaining unassigned spectrum.⁶ Similarly in March, the FCC held an auction for terrestrial wireless licenses in the 24 GHz band (despite some controversy regarding the effects commercial services might have on the adjacent weather band).⁷ The FCC intends to hold an incentive auction this coming December for wireless broadband licenses in the upper 37, 39, and 47 GHz bands.⁸ The Commission also has an open proceeding in which it is considering making portions of the C-Band available.⁹

B. Unlicensed Spectrum

Unlicensed spectrum can be used for a variety of useful services, from wireless microphones in theaters and stadiums to wireless broadband services in remote areas of the country. The FCC has determined that unlicensed uses should be able to share spectrum with licensed services in some places and under certain conditions.

The Commission has made certain spectrum available for unlicensed and shared use in the 3.5 GHz band through a novel, three-tiered spectrum-use co-existence program that automatically coordinates shared Federal and non-federal use of the band.¹⁰ During the

⁵ *Explaining 5G: Millimeter Wave, Sub-6, Low-Band and Other Terms You Need to Know*, AndroidCentral (Jul. 9, 2019) (www.androidcentral.com/explaining-5g-millimeter-wave-sub-6-low-band-and-other-terms-you-need-know).

⁶ Federal Communications Commission, *In the Matter of Transforming the 2.5 GHz Band, Public Draft Report and Order*, WT Docket No. 18-120, FCC-CIRC1907-XX (Jul. 10, 2019).

⁷ Jon Brodtkin, *Ajit Pai Says NOAA and NASA Are Wrong About 5G Harming Weather Forecasts*, Ars Technica (Jun. 13, 2019) (arstechnica.com/tech-policy/2019/06/ajit-pai-says-noaa-and-nasa-are-wrong-about-5g-harming-weather-forecasts).

⁸ Federal Communications Commission, *Notice of Updated 39 GHz Reconfiguration Procedures, Preparation for Incentive Auction of Upper Microwave Flexible Use Services Licenses in the 37 GHz, 39 GHz, and 47 GHz Bands*, Order of Modification, GN Docket No. 14-177, AU Docket No. 19-59, DA 19-397 (May 14, 2019), para. 1.

⁹ Federal Communications Commission, *In the Matter of Expanding Flexible Use of the 3.7 to 4.2 GHz Band*, Order and Notice of Proposed Rulemaking, GN Docket No. 18-122, FCC 18-91 (Jul. 13, 2018), para. 10.

¹⁰ See Federal Communications Commission, *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, GN Docket No. 12-354, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 3959 (2015); see

Broadcast Incentive Auction, the FCC decided to make available for unlicensed use a portion of the 600 megahertz band—the TV White spaces.¹¹ Finally, the Commission is considering making the 6 GHz band available for unlicensed or shared use.¹² The 6 GHz band is currently used for non-federal services, including public safety, coordination of railroad train movement, and control of natural gas and oil pipelines, among others.¹³ The FCC has yet to complete that rulemaking.

II. TELECOMMUNICATIONS SUPPLY CHAIN SECURITY ISSUES

United States communications service providers rely heavily on equipment and services manufactured and provided by foreign companies. The increasingly globalized market for telecommunications equipment and services has increased competition and opened the door to cheaper goods for consumers but poses new challenges for the United States, particularly for ensuring the security of the telecommunications supply chain.

Given the pivotal role that private communications networks serve in connecting U.S. critical infrastructure functions, American networks are appealing targets for foreign adversaries. The United States, therefore, has a clear interest in mitigating threats posed by vulnerable communications equipment and services.

In particular, the United States identified individual Chinese telecommunications firms, including Huawei Technologies Co. Ltd (Huawei) and its affiliates, as posing significant threats to U.S. commercial and security interests.¹⁴ Their susceptibility to state influence over business operations results in China having "the means, opportunity, and motive to use telecommunications companies for malicious purposes," such as espionage and cyberattacks.¹⁵ In April 2018, the U.S.-China Economic and Security Review Commission found that the

also Federal Communications Commission, *In the Matter of Promoting Investment in the 3550-3700 MHz Band*, GN Docket No. 17-258, FCC 18-149 (Oct. 24, 2018), para. 3.

¹¹ Federal Communications Commission, *Unlicensed Operations in the Television Bands, Repurposed 600 MHz Band, 600 MHz Guard Bands and Duplex Gap, and Channel 37*, Report and Order, ET Docket No. 14-165, GN Docket No. 12_268, 30 FCC Rcd 9551 (2015).

¹² Federal Communications Commission, *In the Matter of Unlicensed Use of the 6 GHz Band and Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz*, Notice of Proposed Rulemaking, ET Docket No. 18-295, GN Docket No. 17-183, FCC 18-147 (Oct. 24, 2018), para. 9.

¹³ *Id.*

¹⁴ Department of Commerce, *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List* (May 15, 2019) (press release).

¹⁵ House Permanent Select Committee on Intelligence, *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Cong. (Oct. 8, 2012).

Chinese government has "invested significant state capital and influence" on state-owned enterprises to strategically place these companies in the U.S. telecommunications supply chain.¹⁶

Large telecommunications companies with sophisticated network security operations and significant capital generally have avoided installing and using Huawei and other suspect foreign equipment in their networks.¹⁷ Moreover, Federal agencies have actively reached out to large carriers to express concerns when carriers have considered purchasing suspect equipment.¹⁸ In contrast, some smaller carriers with more limited resources and less sophisticated security operations have purchased and installed Huawei, and other suspect foreign equipment, in their networks either because the equipment was less expensive or they were unaware of the security risk, or both.¹⁹

On May 15, 2019, the White House issued an Executive Order prohibiting "any acquisition, importation, transfer, installation, dealing in, or use of any" information or communications technology involving equipment developed through foreign adversaries.²⁰ The same day, the Department of Commerce's Bureau of Industry Security announced it would add Huawei and its affiliates to its Entity List, limiting their ability to access U.S. exports.²¹

III. LEGISLATION

A. H.R. 4462, the SHARE Act of 2019

Reps. Doyle (D-PA) and Latta (R-OH) introduced in the House on September 24, 2019, H.R. 4462, the "Studying How to Harness Airwave Resources Efficiently Act of 2019" or the "SHARE Act". The SHARE Act would require NTIA, in consultation with the FCC, to establish a spectrum sharing research and development program to explore new ways for Federal entities to share and inventory spectrum with other Federal entities. The legislation would authorize an appropriation to NTIA in the amount of \$50 million to establish the spectrum sharing research and development program. It would also require the FCC to submit a report to Congress on how

¹⁶ U.S.-China Economic Security Review Commission, *Supply Chain Vulnerabilities from China in US Federal Information and Communications Technology* (Apr. 2018).

¹⁷ See, e.g., Paul Mozur, *AT&T Drops Huawei's New Smartphone Amid Security Worries*, the New York Times (Jan. 9, 2018) (www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html).

¹⁸ See, e.g., Todd Shields, *Locke Says Sprint's Chief Was Called About Huawei Bid Concerns*, Bloomberg (Dec. 7, 2010) (www.bloomberg.com/news/articles/2010-12-07/commerce-s-locke-says-sprint-s-chief-was-called-about-huawei-bid-concerns).

¹⁹ See, e.g., Cecilia Kang, *Huawei Ban Threatens Wireless Service in Rural Areas*, the New York Times (May 25, 2019) (www.nytimes.com/2019/05/25/technology/huawei-rural-wireless-service.html).

²⁰ Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019) (published May 17, 2019).

²¹ Department of Commerce, *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List* (May 15, 2019) (press release).

to improve and expand the spectrum sharing techniques developed for the 3.5 GHz band and consider their applicability to other bands, including 3.1 GHz to 3.55 GHz and 7.1 GHz to 8.4 GHz.

B. H.R. 4459, the Secure and Trusted Communications Networks Act

Chairman Pallone (D-NJ), Ranking Member Walden (R-OR), Rep. Matsui (D-CA), and Rep. Guthrie (R-KY) introduced in the House H.R. 4459, the “Secure and Trusted Communications Networks Act” on September 24, 2019. The Secure and Trusted Communications Networks Act instructs the FCC to develop and maintain a list of communications equipment and services that pose an unacceptable risk to national security and prohibits the use of Federal funds to purchase, rent, lease, or otherwise obtain such equipment and services. The bill also establishes the Secure and Trusted Communications Reimbursement Program to assist communications providers with the costs of removing prohibited equipment and services from their networks and replacing prohibited equipment with more secure communications equipment and services.

C. H.R. 4461, the Network Security Information Sharing Act

Reps. Kinzinger (R-IL) and Doyle (D-PA) introduced in the House the bill H.R. 4461, the “Network Security Information Sharing Act” on September 24, 2019. The Network Security Information Sharing Act directs the Secretary of Homeland Security, in cooperation with the Director of National Intelligence (DNI), the Director of the Federal Bureau of Investigation, NTIA, and FCC, to establish a program to share supply chain security risks with advanced communications service providers and trusted suppliers of telecommunications equipment and services.

D. H.R. 2063, the E-FRONTIER Act

Reps. Cárdenas (D-CA), Brooks (R-IN), Vela (D-TX), and Banks (R-IN) introduced in the House the bill H.R. 2063, the "Eliminate From Regulators Opportunities to Nationalize The Internet in Every Respect Act" (E-FRONTIER Act) on April 3, 2019. The E-FRONTIER Act would prohibit the President or any Federal agency from constructing or operating broadband networks or providing wholesale or retail service on a broadband network without prior authorization from Congress.

E. H.R. 2881, the Secure 5G and Beyond Act

Reps. Spanberger (D-VA), Stefanik (R-NY), Slotkin (D-MI), Rooney (R-FL), O’Halloran (D-AZ), and Brooks (R-IN) introduced in the House H.R. 2881, the "Secure 5G and Beyond Act" on May 21, 2019. The Secure 5G and Beyond Act directs the President to develop the "Secure Next Generation Mobile Communications Strategy" in consultation with the heads of the FCC, NTIA, and Department of Homeland Security, as well as the DNI and Secretary of Defense.

The Secure Next Generation Mobile Communications Strategy is intended to: (1) ensure the security of 5G communications systems and infrastructure in the United States; (2) assist mutual defense allies and strategic partners in maximizing the security of 5G networks and infrastructure in their countries; and (3) protect the competitiveness of U.S. companies, the

privacy of American consumers, and the integrity of standards-setting bodies against political influence.

F. H.R. 4500, the Promoting United States Wireless Leadership Act of 2019

Reps. Walberg (R-MI) and Dingell (D-MI) introduced H.R. 4463, the "Promoting United States Wireless Leadership Act" on September 26, 2019. The Promoting United States Wireless Leadership Act directs NTIA to encourage participation by trusted American companies and other stakeholders in standards-setting bodies, and to offer technical assistance to such stakeholder that do elect to participate, in the course of developing standards for 5G networks and future generations of communications networks.

G. H. Res. 575, Expressing the sense of the House of Representatives that all stakeholders in the deployment of 5G communications infrastructure should carefully consider and adhere to the recommendations of "The Prague Proposals."

Reps. Flores (R-TX) and Soto (D-FL) introduced in the House the resolution H. Res. 575 on September 24, 2019. This resolution expresses the sense of the House of Representatives that stakeholders involved in the deployment of 5G communications infrastructure should consider adherence to the international security recommendations adopted at the Prague 5G Security Conference in May 2019, known as "The Prague Proposals." The resolution also encourages the President and Federal agencies to promote trade and security policies on the international stage that are consistent with "The Prague Proposals."

IV. WITNESSES

The following witnesses have been invited to testify:

John Nettles

President
Pine Belt Wireless

Harold Feld

Senior Vice President
Public Knowledge

Dean R. Brenner

Senior Vice President, Spectrum Strategy & Tech Policy
Qualcomm Incorporated

Bobbie Stempfley

Managing Director, CERT Division
Software Engineering Institute
Carnegie Mellon University