Testimony of Harold Feld
Senior Vice President
Public Knowledge

Before the
U.S. House of Representatives
Committee on Energy & Commerce
Subcommittee on Communications & Technology

"Legislating to Secure America's Wireless Future"

Washington, DC
September 27, 2019

HEARING ON
"LEGISLATING TO SECURE AMERICA'S WIRELESS FUTURE"

Harold Feld, Senior Vice President
Public Knowledge

Chairman Doyle, Ranking Member Latta, thank you for inviting me to testify here today. Public Knowledge is pleased to endorse the SHARE Act. Investment in Federal spectrum sharing will have enormous advantages to the federal government and to commercial use of spectrum. Effective dynamic management will do more than free up federal spectrum for auction or open up new federal spectrum for unlicensed access. Technology developed as a result of the SHARE Act will enable federal users to dynamically access better quality spectrum on an as needed basis in a more efficient manner, creating a win for federal users. At the same time, study of the CBRS band will move us closer to the ability to accommodate a mix of priority federal users, licensed interference-protected commercial users, and unlicensed users in the same frequency bands – the Holy Grail of efficient spectrum use.

Public Knowledge is also pleased to support the "Promoting United States Leadership Act of 2019" (PUSLA). Public Knowledge believes strongly that participation by civil society in international standards bodies will dramatically improve the standards process for all. It will also help protect against the use of standards bodies for illegal collusion – an allegation that has emerged from time to time as a consequence of the closed nature of standards bodies. Public Knowledge also supports the Resolution by Mr. Flores on the Prague Protocols as common sense security recommendations for 5G networks.

Public Knowledge generally supports the concepts of the "Secure and Trusted Communications Act of 2019" (STCA) and the "Network Security Information Sharing Act of 2019" (NSISA). However, we recommend several changes to improve the STCA. STCA requires several modifications for due process purposes, such as a mechanism to challenge inclusion on the covered list and a mechanism to seek removal from the covered list. We also believe that reimbursement should not be limited to equipment purchased before August 2018 – especially if new providers are added to the covered list.

We take no position on the "Secure 5G and Beyond Act of 2019," in our testimony.

Finally, we oppose the E-FRONTIER Act as unnecessary and a potential source of negative unintended consequences. The Federal Government cannot build a new network without an appropriation from Congress. This provides more than adequate protection in the event that a future administration should ever seek to move beyond consideration of a national network. On the other hand, the federal government has numerous communications assets – such as spectrum and fiber – which may be of great value if made accessible to the public in emergencies or for rural broadband. The law as written would potentially prohibit any sort of public/private partnership, spectrum sharing agreement, or emergency provision of services. Given the ability of Congress to refuse to appropriate money for any unwanted federal activity, the more prudent course is to simply maintain the status quo.

I address details as to the SHARE Act, PUSLA, NSISA, STCA, and E-FRONTIERS below.

The SHARE Act of 2019 Would Create A Much-Needed Revolution In How Government Manages Spectrum To The Benefit of Federal Users As Well As Commercial users.

The SHARE Act would promote the development of new spectrum technology to allow federal agencies to share spectrum on a more dynamic basis. This would potentially revolutionize spectrum management for federal agencies. At present, federal agencies allocate spectrum in essentially the same way we have for decades, and the sad state of the Communications Act in this regard reflects our failure to acknowledge the march of technology. For example, Section 323 of the Communications Act requires that, in the event of interference between government users and commercial users, government users shall "transmit radio communications or signals only during the first 15 minutes of each hour."[1] While this was cutting edge 'time-division multiplexing' in 1927 when the statue was first written, we can surely do better today.

Dynamic sharing, once proven and reliable, would allow the federal government to move away from the existing allocation process that requires agencies to seek specific allocations of spectrum and invest in equipment limited to the specific frequencies allocated for the federal agency. This means that agencies may face spectrum constraints at critical times, while retaining unused spectrum allocations against future need. This problem is often further aggravated by the age and inefficiency of equipment. To make matters worse, each federal agency is responsible for its own equipment from its own budget. Rather than think of federal users as one giant user able to achieve economies of scale and match spectrum capacity needs with the specific mission, we currently atomize our spectrum policy across the federal government. This locks in historic allocations,

[1] 47 U.S.C. §323(b).

drives up overall equipment cost, and generally interferes with the ability to supply all branches of government with the reliable, cutting edge equipment needed to successfully complete operations in the digital age.

By creating a test bed for spectrum sharing among federal users – and by studying the CBRS system for accommodating federal priority users with commercial users – we can take the first step forward in modernizing federal spectrum management. It is extremely unfortunate, not to mention bad policy, to simply view enhanced federal sharing capacity as a means of clearing more spectrum for auction, or for finding ways to accommodate federal users and unlicensed users to co-exist. While it is inevitable that enhanced spectrum efficiency on the part of the government will provide such opportunities for expanded commercial use, the real value of the SHARE Act for the future will be technology that provides to all agencies access to more and better spectrum on an as needed basis while reducing the overall federal spectrum footprint.

Enhancing Federal Spectrum Sharing Will Improve National Security and Our Ability To Work With Allies on Humanitarian Missions.

As members of the Subcommittee are aware, the activation in Mexico of a new commercial cellular network has created significant interference issues with public safety licensees operating along the border.[2] This is a dramatic example of the problems faced by federal and commercial users with regard to frequency coordination with other countries. Although participation in the International Telecommunications Union (ITU) is

[2] *See* Vic Kolenc, "Mexico Cellular Network Is Problem for U.S. Phone Service, El Paso Emergency Responders," El Paso Times (September 20, 2019). Available at: https://www.elpasotimes.com/story/money/business/2019/09/20/mexico-cellular-network-disrupts-wireless-communications-united-states-mexico-border/2347529001/ (last visited September 24, 2019).

helpful for harmonizing global use, it does not prevent countries from adopting different band plans or different frequency allocations.

Developing ways to share spectrum without mutual interference will directly benefit federal users on the borders or when deployed abroad. Whether spectrum sharing techniques and technologies developed pursuant to the SHARE Act require mutual cooperation, or are simply "plug and play" by federal users to avoid interference, we can anticipate significant spin off benefits in addressing problems such as those currently plaguing emergency responders along the border with Mexico. These technologies will also provide ways for our military or other federal responders – such as aid personnel dispatched for disaster relief – to operate in coordination with host countries.

CBRS Represents A Major Breakthrough for Sharing Between Federal Users, Licensed Users and Unlicensed Users That Points The Way for Future Cooperation.

Changes to spectrum access assignment happen only slowly, and with great resistance. Formalizing the process of permitting unlicensed spectrum underlays took most of the 1980s, for example. Ultra-Wideband (UWB) took years, and is only just now potentially coming into wide adoption with Apple's decision to include an UWB chip in the iPhone 11.[3]

All of this makes the relatively rapid adoption and investment in Commercial Broadband Radio Service (CBRS) that much more remarkable. CBRS represents the first effort to develop a technology capable of accommodating federal users, exclusive commercial licensed users, and unlicensed users in the same general set of frequency

[3] *See* Jason Snell, "The U1 Chip In the iPhone 11 is the Beginning of an Ultra Wideband Revolution," Six Colors (September 13, 2019). Available at: https://sixcolors.com/post/2019/09/the-u1-chip-in-the-iphone-11-is-the-beginning-of-an-ultra-wideband-revolution/
(last visited September 24, 2019).

bands on a dynamic basis.[4] Although the FCC finalized rules for the band in 2015. The determination of the current FCC to conduct a new rulemaking and make substantive changes to the rules for allocating the Priority Access Licenses (PALs) created considerable, unnecessary delay. Nevertheless, the approval by the FCC last week of 5 spectrum access system (SAS) providers has now opened the door to a projected billion dollars in investment by 2023.[5]

The early success of CBRS – despite significant initial resistance and a two-year delay imposed by the current FCC – highlights the importance of studying it as a model for future spectrum sharing. In particular, CBRS has empowered users to access spectrum reserved for licensed users until the licensees actually activate their systems – a function called "use or share." For over a decade, wireless experts and rural advocates have explained that "use or share" technology holds great promise in bringing wireless broadband to rural areas neglected by licensees. As a general rule, licensees focus deployment in areas of greater population density, leaving communities with much sparser population densities with either subpar service or no service at all. Use or share allows small wireless ISPs (WISPs) or even individuals to deploy affordable, off-the-shelf technology in areas that licensees have no interest in serving. Nevertheless, incumbent licensees have strenuously resisted efforts to incorporate use or share into license rules.

---

[4] Technically, the "General Authorized Access" (GAA) is licensed by rule under 47 U.S.C. §307(e). As a practical matter, however, it functions for users in the same way as unlicensed access.

[5] Kendra Chamberlain, "CBRS RAN Market Investment to Surpass $1B by 2023: Dell'Oro Report," Fierce Wireless (March 22, 2019). Available at: https://www.fiercewireless.com/wireless/cbrs-ran-market-investments-to-surpass-1b-by-2023-dell-oro-report
(Last visited on September 24, 2019).

The CBRS deployment will prove the technical feasibility of use or share, and its value to both unserved communities and to licensees. In the event the licensee wishes to deploy in the area, the existing users will default back to the available GAA, so that no existing network will lose access. Crowded urban areas will provide valuable data on the usefulness and feasibility of use or share in areas where licensed deployment can be expected to be swift and intense, while rural areas will demonstrate the value of keeping spectrum in productive use despite the absence of licensee investment.

PUSLA Will Improve the International Standards Process And Promote Innovation, Competition and Consumer Protection.

Standards can fix policy just as easily as any rulemaking. The decisions that are made in standards bodies impact consumer protection concerns such as personal privacy. But often no one is present in these standard meetings to raise these concerns. In addition, because standards bodies bring together industry rivals, they may become avenues for collusion. As Adam Smith warned: "People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public or a contrivance to raise prices."[6] On multiple occasions rumors have circulated that large incumbents have attempted to manipulate the standard setting process to the detriment of smaller competitors.[7] To be clear, we do not suggest that the standard setting process is generically suspect or a bad thing. To the contrary, industry standards developed through recognized standard-setting bodies play an important role in promoting competition and developing numerous improvements and innovations that benefit consumers. But even

[6] The Wealth of Nations, Book 1 Chapter X.
[7] *See, e.g.,* Cecilia Kang, "U.S. Investigating AT&T and Verizon Over Wireless Collusion Claims," New York Times (April 20, 2018). Available at: https://www.nytimes.com/2018/04/20/technology/att-verizon-investigate-esim.html (Last accessed September 24, 2019).

without concerns about possible anti-competitive or anti-consumer conduct, it is important for a wide range of stakeholders to be represented in the major international standard setting bodies to protect American interests and improve the quality of standard setting generally.

Additionally, involvement of civil society in ITU settings has proven important to advancing the national goals of the United States in defending Internet freedom and enhancing the general credibility of the United States delegation. I participated with the United States delegation to the World Conference on International Telecommunications (WCIT) in 2012, and can say from personal experience that the integration of civil society stakeholders and industry stakeholders enormously improved our ability to influence outcomes.

PUSLA offers an important first step in providing access to technical knowledge necessary to participate in international standard setting bodies. This could be improved by a more explicit commitment to civil society engagement, and by making funds available to cover dues and travel costs for representatives from civil society or small businesses. Even without these, however, Public Knowledge supports PUSLA and urges the Subcommittee and full Committee to move it forward.

The NSISA and STCA Underscore the Need To Acknowledge The Reality That Broadband and VOIP Are Title II Communications Services.

That Congress needs to pass special legislation to protect our critical communications infrastructure should highlight one thing clearly. Broadband is a Title II telecommunications service. Time and again, Congress finds itself reinventing provisions of the Communications Act using cumbersome circumlocutions to include voice over IP (VOIP) and broadband because the same logic that compelled inclusion of these concepts

in the Communications Act apply with equal force to the critical communications infrastructure of today. Just as the Communications Act makes the reliability and security of communications infrastructure central to the mission of the FCC, we find ourselves updating this concept for cybersecurity. Despite the insistence that broadband and VOIP networks are so radically different from "communications" that they should not be included in the same statutory framework, we find ourselves once again – as we did with universal service, pole attachments, and just about every other provision related to telecommunications networks – classing broadband and VOIP with other communications providers and applying the same necessary safeguards.

Congress should simply acknowledge this reality and restore broadband to Title II classification (and clarify that interconnected VOIP is also Title II). The House already took this step earlier this year. It is time for the Senate to pass the Save the Internet Act. Indeed, in a fine irony, the FCC Notice of Proposed Rulemaking referenced in STCA (proposing to prohibit USF recipients from purchasing equipment or services from covered entities) cites as its primary source of authority 47 U.S.C. §201(b).[8] If anything should highlight the obstinate folly of refusing to recognize the value of Title II classification and its relevance to broadband and VOIP, one would think that the current Commission's continued reliance on Title II generally and Section 201(b) specifically, to address broadband security vulnerabilities would be it.

NSISA's Information Sharing Regarding Communications Supply Chain Risks Is Useful for Shoring Up Key Vulnerabilities in Network Equipment and Devices.

[8] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, *Notice of Proposed Rulemaking* Docket No. 18-89 ¶35.

As cybersecurity expert Bruce Schneier warned just this week, every element of the supply chain is vulnerable – and the majority of attacks come from criminals not state-sponsored companies.[9] We have seen an explosion of ransomware against national and state governments. Security holes in devices have been exploited to bring down significant portions of the Internet. Exploitable weaknesses can come not only from the manufacturers or service providers under state control. As Schneier explains, open source programs can be manipulated by users, counterfeit chips can be introduced by bad actors, and patches to proprietary software can hide backdoors or other malware.

The NSISA provides a useful mechanism for communicating threats to our critical communications infrastructure gathered from foreign intelligence.

STCA Requires Modifications To Adequately Address Future Security Concerns, Ensure That Small Carriers That Act In Good Faith Are Held Harmless.

The STCA lacks important provisions to ensure due process. Because the STCA contains provisions for the FCC to add new companies, on an ongoing basis, the STCA should contain provisions by which an entity proposed for the updated list can challenge the designation before it goes into effect. Additionally, the STCA should require an explicit process for removal from the list. This should apply even to the named companies Section 2(b)(1)(A). We cannot predict today what our relationship will be with China in the future, nor can we predict what the relationship between these companies and the Chinese government will be in the future. But the statute provides no

[9] Bruce Schneier, "Every Part of the Supply Chain Can Be Attacked," New York Times (September 25, 2018). Available at: https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html?fbclid=IwAR1PneYnY2wD4AOHh83NiJyIM6ToSDLRhWEgL8SL21pX9u2T_y0Y7PEDwp4
(Last accessed September 25, 2019).

authority to remove any company, let alone the two companies specifically named in the statute.[10]

We do not believe that reimbursement should be limited solely to equipment purchased before August 14, 2018. It is unreasonable to presume that small providers constantly read the Federal Register and are aware of every FCC proceeding. This is particularly true for broadband providers, who have not generally been regulated by the current FCC. But even if providers are aware of the ongoing FCC proceeding, there was no reason to assume that the FCC would ultimately act on the proceeding. Furthermore, no provider potentially eligible for reimbursement could have foreseen that Congress would provide for reimbursement but punish providers who made the rational economic decision to keep buying low-priced equipment until the FCC told them to stop.

Finally, the statute as written would make it impossible for providers to receive reimbursement in the event the Commission identifies any future covered entities. The statute recognizes that new situations may come to light which would make it hazardous to buy equipment or services that may not even exist today. Under the statute, carriers will need to replace equipment from these newly identified threats. Given that the statute maintains the availability of funds for ten years, funds may be available to help these good faith purchasers ensure their networks comport with national security

[10] We note that specifically naming a company in the statute as subject to a specific penalty raises concerns that the statute will be considered an unlawful Bill of Attainder. Recent case law suggests that security measures such as this against companies that are at least partially owned or controlled by a foreign power may not constitute a Bill of Attainder but a reasonable security measure. *See Kapersky Lab, Inc. v. DHS*, 311 F. Supp. 3d 187 (D.D.C. 2018). Because this lies outside the scope of our expertise, Public Knowledge expresses no opinion on the matter.

determinations. It makes no sense to prohibit future injured parties from applying for reimbursement for expenses they could not predict would be problematic.

Securing our nation's critical infrastructure is our common responsibility. We should not ask small providers that are dependent on federal grants to provide service to rural America to bear the cost. Any provider that purchased equipment of services in good faith should be eligible to receive funding to replace listed equipment.

E-FRONTIER Is Unnecessary And Will Have Negative Unintended Consequences.

The E-FRONTIER Act, and its companion bill in the Senate, appear to be a direct response to press reports about an early-2018 recommendation within the Trump Administration to build a nation-wide, federal 5G network. This proposal has been roundly repudiated by the Trump Administration – most notably at a public event on 5G networks where he shared the podium with FCC Chairman Ajit Pai.[11] The FCC's Democratic Commissioners have likewise dismissed the proposed national network as misguided.[12] Nor could any Administration, now or in the future, build such a network without an appropriation from Congress. Like the hypothetical network the statute would prohibit, the E-Frontier Act is a solution in search of a problem.

Unfortunately, passing legislation is not merely a symbolic act. It has real, unintended consequences. The federal government provides numerous loans and grant programs. Without a review, it is likely that the E-FRONTIER Act will create needless

[11] Aaron Pressman, "Forget Rural Internet – This Was the Real Agenda at Trump's 5G Wireless Event," Fortune (April 12, 2019). Available at: https://fortune.com/2019/04/12/trump-ajit-pai-5g-wireless-auction-rural-internet/ (Last accessed September 25, 2019).

[12] Harper Neidig, "FCC Chair Opposes Nationalizing 5G Network," The Hill (January 29, 2018). Available at: https://thehill.com/policy/technology/371184-fcc-chair-comes-out-against-nationalizing-5g-network (Last accessed September 25, 2019).

confusion. For example, if the Department of Housing and Urban Development funds broadband in federal housing, would such a program violate the E-Frontier Act? Would operation of a network designed to bring service to rural hospitals, or to military housing outside a military base, constitute a "wholesale" or "retail" network? How will E-FRONTIER impact RUS recipients? Given the sweeping language of the E-FRONTIER Act, the enormous number of potential federal grants, and the increasing centrality of broadband in everything from housing to healthcare, the likelihood of some undesired negative consequence, such as discouraging valuable projects or encouraging grant challenges, seems almost certain.

Even worse, the E-FRONTIER Act will potentially curtail efforts to use federal assets such as spectrum or fiber to assist in natural disasters or provide broadband to rural areas. Consider the following examples. A massive hurricane sweeps away commercial networks, but federal fiber remains usable. The federal government wants to make the capacity available for wholesale use by carriers until they can restore their own service. The plain language of the E-FRONTIER Act would prevent any such helpful use of federal fiber or other communications assets. Or imagine if a military installation or federal research facility pulls fiber into an isolated rural community. Would we really want to prohibit any creative way in which the community might leverage federal fiber to close the local digital divide? Or imagine a federal agency contracts with a company to use federal spectrum, allowing the company to provide commercial service over any excess capacity. Would this constitute a federal wholesale or retail network under the sweeping language of the E-FRONTIER Act.

No one of these possibilities is particularly likely in the near term, but the likelihood that the E-FRONTIER Act will unintentionally diminish flexibility in federal projects, federal contracting, or federal disaster response is very real. Even if the risk seems remote, why take any risk at all? No federal network is planned, nor can any proceed without federal funding. If such a network ever did seem like a substantial possibility, Congress could pass targeted legislation then.

CONCLUSION

No one can argue that Congress should ignore the threats to our critical infrastructure or the importance of maintaining U.S. leadership in wireless technology. As discussed above, the SHARE Act and PUSLA are important investments in our wireless future. NSISA and STCA address critical network security needs, but should be modified as discussed above. The E-FRONTIER Act, however, is both unnecessary and creates unintended consequences.

Thank you and I am prepared to answer any questions at this time.