

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Revision of Rules and Requirements)	WT Docket No. 96-86
For Wireless Priority Service)	
)	
To: Public Safety and Homeland Security Bureau)	

COMMENTS OF TECHFREEDOM

TechFreedom, pursuant to Sections 1.415 and 1.419 of the Commission’s rules (47 C.F.R. §§ 1.415 & 1.419), submits these Comments in the above-referenced proceeding in response to the Commission’s Public Notice of August 13, 2018.¹ In the Public Notice, the Commission seeks comment on the National Telecommunications and Information Agency (“NTIA”) Petition for Rulemaking, filed July 9, 2018, requesting that the FCC open a proceeding to update the rules and requirements for Priority Access Service (PAS), now commonly known as Wireless Priority Service (WPS).²

I. About TechFreedom

TechFreedom is a non-partisan think tank dedicated to promoting the progress of technology that improves the human condition. To this end, we seek to advance public policy that makes experimentation, entrepreneurship, and investment possible, and thus unleashes the

¹ *Public Notice*, DA 18-485, released August 13, 2018.

² NTIA Petition for Rulemaking in WT Docket No. 96-86, filed July 9, 2018 (hereinafter “NTIA Petition”).

ultimate resource: human ingenuity. Wherever possible, we seek to empower users to make their own choices online and elsewhere.

II. Discussion

A. Introduction

TechFreedom applauds NTIA for filing its Petition for Rulemaking, and urges the FCC to open a proceeding to explore updating the WPS rules as they related to providing services to National Security and Emergency Preparedness (NS/EP) users.³ As NTIA points out, the FCC hasn't undertaken a comprehensive review of the interplay of public safety communications and the both the wired and wireless communications networks since shortly after September 11, 2001 attacks.⁴ Especially given how much public safety communications “rides” on the commercial networks, and how integrated data communications have become integrated into public safety communications, a comprehensive federal approach to these issues is long overdue. Unless the FCC updates WPS rules, there is significant danger that states may try to establish their own rules, citing a need to “protect public safety.” Such state regulation of the inherently interstate medium that is the Internet would raise grave constitutional concerns about federalism.

B. The WPS Rules Do Not Involve Net Neutrality Regulations

First and foremost, the FCC must make clear that the WPS and other rules related to public safety communications must be free of the partisan bickering that has consumed all the oxygen in Washington, D.C. in the name of “net neutrality.”⁵ NTIA raises this issue in its

³ See 47 C.F.R. Part 64, App. B.

⁴ NTIA Petition, at 4.

⁵ TechFreedom has been involved in the net neutrality debate since its inception in 2011. See, e.g., Comments of TechFreedom, *In the Matter of Notice of Proposed Rulemaking-Restoring Internet Freedom*, WC Docket No. 17-108 (Aug. 30, 2017), http://docs.techfreedom.org/TechFreedom_Reply_Comments_on_Open_Internet_Order.pdf; Berin Szóka,

Petition as well.⁶ The need to promote public safety is real. So, too, are NTIA’s concerns about the current limitations of the WPS rules, as recent events suggest that those in favor of heavy-handed Title II regulation of our communications networks will use any news hook, even concern about public safety communications, as an opportunity to justify regulatory micromanagement of the Internet.

Net neutrality activists are having a political field day with an August 22, 2018 *Ars Technica* report that Verizon had “throttled” the data usage of the Santa Clara County Fire Prevention District (FPD), one of the California counties fighting the largest wildfire in the state’s history.⁷ Proponents of Title II regulation have claimed that that the FCC’s 2015 rules would have prevented Verizon from “restricting” the fire department’s Internet service.⁸ In fact, the 2015 Open Internet Order’s no-throttling rule clearly, and explicitly did not apply to the issue in the FPD case: customer confusion over service plans that offer more data but with the condition that a speed restriction kicks in at some point.⁹ The FPD chose a data plan (4G speeds

Only Congress, Not the FCC, Can Fix Net Neutrality, WIRED (May 17, 2017), <https://www.wired.com/2017/05/congress-not-fcc-can-fix-net-neutrality/>; Tech Policy Podcast, *Future of Internet Regulation* (w/ FCC Chairman Ajit Pai) (2017), <http://podcast.techfreedom.org/e/172-future-of-internet-regulation-w-fcc-chairman-ajit-pai/> (last visited Aug. 28, 2018); Brief for Petitioner for The State of Tennessee, et. al, *Tennessee v. F.C.C.*, 832 F.3d 597 (2016) (No. 15- 3291; 15-3555) (2015), http://docs.techfreedom.org/TechFreedom_Amici_Brief_Section706.pdf.

⁶ NTIA Petition, at 9-11.

⁷ See Jon Brodtkin, Fire dept. rejects Verizon’s “customer support mistake” excuse for throttling, *ARS TECHNICA* (Aug. 22, 2018), <https://arstechnica.com/tech-policy/2018/08/fire-dept-rejects-verizons-customer-support-mistake-excuse-for-throttling/>.

⁸ Gigi Sohn, *Verizon couldn’t have restricted Santa Clara County’s Internet service during the fires under net neutrality*, *NBC News* (Aug. 24, 2018), <https://www.nbcnews.com/think/opinion/verizon-couldn-t-have-restricted-santa-clara-county-s-phone-ncna903531>.

⁹ See *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, FCC 17-166 (Jan. 4, 2018) (*Restoring Internet Freedom Order*), http://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0104/FCC-17-166A1.pdf; *In the Matter of Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, ¶ 106 (2015) (JA 3477-8876),

only for the first 25 GB/month, but “unlimited” data after that) that was manifestly unsuited for their needs (up to 300 GB/month of 4G data), and then apparently misunderstood that Verizon’s generous policy of suspending speed restrictions when government users claimed emergency circumstances did not mean the device would be *permanently* exempted from such caps.¹⁰

The FPD has now become the “poster child” for Title II regulation, the story now a key piece of evidence in the appeal of the 2017 Restoring Internet Freedom Order (RIFO).¹¹ In fact, all that happened in that case was a series of human errors and misunderstandings have nothing to do with “throttling” or other net neutrality principles. We have written about this red herring.¹²

TechFreedom is very concerned that this proceeding will become yet another food fight in the name of net neutrality. NTIA has made abundantly clear, however, that without clear protections and immunity from liability, wireless providers will not offer vital public safety communications products, stifling further innovation and endangering the public at large:

In 2000, the Commission recognized that CMRS providers would be unlikely to offer priority services if by so doing they risked liability for violating the Communications Act. Because the voice services then at issue were common carrier services, the principal concern was that provision of priority services only to NS/EP personnel might violate carriers’ nondiscrimination obligations under section 202 of the Act. To remove that potential barrier to offering such services, the Commission declared that if CMRS providers comply with the operating protocols specified in Part 64,

https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf (outlining the rule banning throttling).

¹⁰ See, B. Szóka, “False Alarm: Verizon’s Fire Department Customer Service Fail Has Nothing to Do with Net Neutrality,” August 28, 2018 (<https://medium.com/@BerinSzoka/false-alarm-verizons-fire-department-customer-service-fail-has-nothing-to-do-with-net-neutrality-3b9a2d770e5b>).

¹¹ See, e.g., <https://cdn.arstechnica.net/wp-content/uploads/2018/08/fire-department-net-neutrality.pdf> (Addendum to Brief for Government Petitioners, Mozilla, Co., v. FCC, (No. 18-1051), 2018 WL 3992563 (D.C. Cir. filed Aug. 17, 2018)).

¹² *Supra*, n. 10.

Appendix B, they would be immune, in most circumstances, from liability under section 202.¹³

Going forward, NTIA is equally concerned about the introduction of innovative services that must also be protected from vague claims that they are somehow “unreasonable”:

Allowing provision of next generation voice, data, and video telecommunications and information services on a priority basis presents similar liability concerns that could dissuade WPS providers from offering them. For example, the Commission has not ruled whether interconnected Voice over Internet Protocol (VoIP) services are “information services” or “telecommunications services.” Thus, a CMRS provider offering priority or preemptive VoIP services only to NS/EP personnel could face the risk of litigation and potential liability for violating section 202.¹⁴

TechFreedom agrees that providers must be immunized from collateral claims of liability when they undertake to provide vital services to NS/EP users. We urge the FCC to clarify the extent that providers are immune from claims of discrimination or unreasonableness under the Communications Act.

C. The FCC Must Not Allow States to Interject Their Own Public Safety Communications Regulations

The effort to reinstate the 2015 Open Internet Order’s Title II regulations is not limited to federal court challenges of the RIFO. As we have written elsewhere,¹⁵ some thirty-six (36) states, have attempted to reinstate the 2015 Title II Order at the state level, either through legislation or executive order. Depending on how those state-level regulations define “throttling,” providers complying with federal WPS rules that allow providers to preempt or degrade commercial traffic to prioritize NS/EP communications may find themselves in violation of state laws. The fear of

¹³ NTIA Petition, p. 8 (footnotes omitted).

¹⁴ *Id.* at 9 (internal footnotes omitted).

¹⁵ See Graham Owens, Federal Preemption, the Dormant Commerce Clause, and State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail, Forthcoming (July 19, 2018), <https://ssrn.com/abstract=3216665>.

legal liability — potentially including *criminal* liability under some state laws¹⁶ — and arbitrary enforcement by state attorney generals will deter providers from offering public safety priority communications.

Similarly, providers offering data plans (including to NS/EP users) that reduce speeds once certain data caps are reached, which are perfectly legal under both the 2015 *Title II Order* and the *RIFO*,¹⁷ may find themselves in violation of state net neutrality laws and policies. If left unchecked, the marketplace will naturally react with either (a) the total withdrawal of services to NS/EP users, or (b) the requirement that such users, since they can't be “throttled,” will be required to pay (far) more. Either way, public safety will suffer so politicians can score points.

The FCC in this proceeding, therefore, must make abundantly clear that the WPS rules are a creature of federal communications policy and that states are preempted from adopting any rules that conflict with the federal regulations.¹⁸ While TechFreedom is confident that such

¹⁶ See, e.g., S. 460, 2017-2018 Leg., Reg. Sess. (Cal. 2018) (prohibiting “a state agency from contracting with an [ISP] for the provision of [BIAS] unless that provider certifies under penalty of perjury that it will not engage in specified activity”).

¹⁷ See *Protecting and Promoting the Open Internet*, WC Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, ¶ 153 (2015) (*Title II Order*) (“Usage allowances place limits on the volume of data downloaded by the end user during a fixed period. Once a cap has been reached, the speed at which the end user can access the Internet may be reduced to a slower speed, or the end user may be charged for excess data. Usage allowances may benefit consumers by offering them more choices over a greater range of service options, and, for mobile broadband networks, such plans are the industry norm today, in part reflecting the different capacity issues on mobile networks”); See also *Restoring Internet Freedom Order (“RIFO”)*, 33 FCC Rcd 311, ¶ 82 (2017) (“Given the unresolved debate concerning the benefits and drawbacks of data allowances and usage-based pricing plans, we decline to make blanket findings about these practices and will address concerns under the no-unreasonable interference/disadvantage on a case-by-case basis”).

¹⁸ We can imagine any number of horror stories that could result from a patchwork set of state regulations related to public safety communications that might differ from state to state. Imagine a forest fire around Lake Tahoe, where providers are called upon to provide public safety communications to fire departments from both California and Nevada. Will lawyers need to be parachuted into the area to figure out which state law applies and whether the plans offered are compliant in both states, one, or neither?

conflicting rules would be overturned on preemption and Dormant Commerce Clause grounds,¹⁹ the uncertainty that would be injected into the marketplace as such litigation plays out across the country would not be in the public interest, as providers would hesitate to voluntarily provide priority services until the controversy is resolved.

D. The FCC Should Move Slowly Before Adopting Rules That Allow Providers to Preempt (Terminate) or Degrade Ongoing Commercial Communications

Currently, the WPS rules do not allow providers to terminate or degrade ongoing calls or data communications. NTIA requests that the FCC modify the rules to allow such conduct in emergency situations.²⁰ TechFreedom supports a study of this proposal, but at this point cannot endorse it. We are concerned that if the public suddenly finds that its important (but non-emergency) communications are disrupted in a time of emergency, the ripple effects on the communications networks could be disastrous. Most importantly, will people whose calls are suddenly cut off during a flood or fire turn instantly to the 911 system and therefore swamp PSAPs reporting the “emergency” of their calls to loved ones being cut off?

Better data are needed from both NTIA and the providers to predict how often calls will be terminated or degraded. A full record needs to be developed in this area. Further, if the FCC is to consider allowing calls to be terminated, it must first explain how the public will be educated as to this fundamental change in their access to the communications networks. The American public is used to an “always on” communications grid. So how will they react to a government policy that allows their calls to loved ones in times of emergency to be cut off in mid-sentence?

¹⁹ See Owens, *supra* note 15, at 4 (finding that “while multijurisdictional regulation—both vertically between Federal and state governments and horizontally among the states—is not unique to regulation of the Internet, the uniquely global nature of the Internet and the FCC’s express preemption statement will render the states’ efforts to impose net neutrality obligations on ISPs invalid upon judicial review.”).

²⁰ NTIA Petition, p. 5.

We think NTIA understates the potential public backlash to this suggested fundamental change in communications policy.²¹

Above all, the FCC must make clear that if it allows providers to preempt or degrade commercial communications, it will *not* allow state and local governments to abuse this capability to preempt the commercial networks — as was done by the Bay Area Rapid Transit (BART) system on August 11, 2011, when it shut down cellular service in four BART stations during a protest.²² There is nothing more antithetical to “public safety” than cutting off the communications grid in order to stifle speech a government doesn’t want to hear.

E. This Proceeding Should Explore Whether There are Fundamental Differences Between Emergency Voice Communications and Emergency Data Communications

The NTIA Petition urges the FCC to allow providers to voluntarily extend priority access from voice and low data communications to all data communications used by NS/EP users.²³

²¹ TechFreedom is also concerned that some of the technical underpinnings to this proceeding are not public. *See, e.g.*, NTIA Petition, p. 5, n.12. “The NS/EP Priority Services Functional Requirements Specification (FRS) is a formal statement of the functional requirements for priority services developed by the OEC. The FRS serves as a basis for service contracts governing the acquisition of priority capabilities within commercial telecommunications networks. DHS/OEC has not made the FRS available to the public. Those wishing to review the FRS may submit a request via email to OEC@hq.dhs.gov. DHS will review all such requests and make a release determination.” *See also* NTIA Petition, p. 15, n. 34. “White House, Information Infrastructure Protection Assurance Group (IIPAG) Convergence Working Group, Report on the Impact of Network Convergence on NS/EP Telecommunications: Initial Findings and FY02/FY03 Programmatic Recommendations (July 2001). This document has not been made public. Those wishing to review the July 2001 Convergence Working Group Report may submit a request via email to OEC@hq.dhs.gov. DHS will review all such requests and make a release determination.” TechFreedom is not a subject matter expert in the details of public safety communications, but nonetheless is concerned as to whether this proceeding may suffer from a lack of transparency. We urge both NTIA and the FCC to make these documents public unless there is a clear national security concern with releasing this information.

²² Press Release, TechFreedom, Courts, Not FCC, Should Protect Free Speech Against Mobile Service Shut-offs (March 2, 2012), <http://techfreedom.org/courts-not-fcc-should-protect-free-speech/>.

²³ NTIA Petition, at 7.

NTIA raises the issue of whether the status of BIAS as an Information Service rather than a Telecommunications Service changes the analysis:

Uncertainty also exists, albeit in a different way, for any broadband Internet access services (BIAS) that CMRS providers may offer as part of WPS. Although the Commission recently determined that such offerings are information services largely exempt from its jurisdiction, that decision does not end federal regulatory oversight of BIAS. As the Commission notes, because most providers of fixed and wireless BIAS have committed not to block or throttle their customers' lawful Internet traffic, those commitments are now enforceable by the Federal Trade Commission (FTC) pursuant to its authority under section 5 of the Federal Trade Commission Act. As a result, if a WPS-participant's offering of priority access to its BIAS service by NS/EP personnel could result in interference with or disruption to the traffic of other BIAS users, the provider could incur litigation costs and potential liability before the FTC.²⁴

The Commission should declare that if a WPS participant offers to qualified NS/EP personnel priority access to its BIAS service consistent with the requirements of Part 64, Appendix B (amended as requested herein), then the Commission would recommend that the FTC forego any action or deny any complaint under section 5. Although that recommendation would not bind the FTC, it would likely reduce significantly the potential for an adverse FTC decision. By so doing, the FCC's declaration would reduce a legal uncertainty that may dissuade a CMRS provider from including BIAS in its WPS offerings.²⁵

TechFreedom agrees with this analysis and believes that the FCC can both establish clear policies in this area as well as work with the FTC to ensure that no "unintended consequences arise from extending the WPS rules to BIAS services. To build on the FCC-FTC Memorandum of Understanding entered into by the two agencies last December,²⁶ we recently recommended to the FTC that the agency issue, after seeking public comment on a draft, a policy statement on

²⁴ *Id.* at pp. 9-10 (footnotes omitted).

²⁵ *Id.* at pp. 10-11 (footnotes omitted).

²⁶ Restoring Internet Freedom FCC-FTC Memorandum of Understanding, § 3 (Dec. 14, 2017), https://www.ftc.gov/system/files/documents/cooperation_agreements/fcc_fcc_mou_internet_freedom_order_1214_final_0.pdf.

how the agency will handle broadband.²⁷ Specifically addressing the issue of public safety in such a policy statement would not technically bind the agency, of course, nor could it bind the state attorneys general who could also bring deception claims under “Baby FTC” acts, but it would make it unlikely that such claims would be brought in the first place — and thus reduce the legal uncertainty that might discourage providers from providing valuable public safety services.

III. Conclusion

A thorough review of the WPS rules is long overdue. TechFreedom looks forward to participating in this proceeding to help develop a record that reflects rational approaches to regulation rather than knee-jerk political battles that produce no public interest benefits.

Respectfully submitted,

TECHFREEDOM

By: _____/s/_____

James E. Dunstan
Berin Szóka
Graham Owens
110 Maryland Ave NE
Suite 409
Washington, DC 20002

Dated: August 28, 2018

²⁷ Comments of TechFreedom, Hearings on Competition & Consumer Protection in the 21st Century: Topic 2: Competition and Consumer Protection Issues in Communication, Information, and Media Technology Networks (Aug. 20, 2018), <http://techfreedom.org/wp-content/uploads/2018/08/ftc-august-2018-workshopcomments-topic-2.pdf>.