May 20, 2020

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20054
Via Electronic Filing

In the Matter of	)	
	)	
Restoring Internet Freedom	)	WC Docket No. 17-108
	)	
Bridging the Digital Divide for Low-Income Consumers	)	WC Docket No. 17-287
	)	
Lifeline and Link Up Reform and Modernization	)	WC Docket No. 11-42

Reply Comments of Richard Bennett, High Tech Forum

Introduction

I[1] am delighted to offer these reply comments to aid the Commission in explaining its reasoning to the Court regarding the consideration for the legitimate needs of public safety embedded in and implied by the *Restoring Internet Freedom Order*.

[1] I am an independent network engineering consultant and policy analyst, presently working at High Tech Forum as editor and founder and as an independent consultant. These remarks are offered in my personal capacity and do not necessarily represent the opinions of any client or sponsor. I have previously offered comments in the "Restoring Internet Freedom Order" docket, WC 17-108, the "Protecting and Promoting the Open Internet" docket, GN 14-28, the "Preserving the Open Internet" and "Broadband Industry Practices" dockets, GN 09-191 and WC 07-52 respectively, and offered testimony at the FCC En Banc Public Hearing on Broadband Network Management Practices in Cambridge on February 25, 2008 as an invited technical expert. My CV is available at https://www.bennett.com/resume.pdf.

Reply Comments

1. Overview

This proceeding is one of many addressing limits to the FCC's ability to enforce unwritten rules. Supporters of the 2015 Title II Order's approach to the regulation of broadband Internet Service providers want the agency to have this power, while exponents of the Restoring Internet Freedom Order prefer the regulatory certainty provided by the traditional view that the Commission must publish a rule before enforcing it. Regardless of how many words we write about prioritization and discrimination, we are fundamentally contesting the issue of unwritten rules.

We've come to this pass because 20 years of discussion of the net neutrality chimera has failed to advance a coherent set of actual rules; prohibitions on blocking, throttling, paid prioritization, and the vague definition of non-Internet data services do not satisfy the Title II side unless the Commission can simply make up additional regulations as it goes along. We are meant to believe that the Commission has the wisdom to evaluate events in real time that it never had the wisdom to predict.

This chapter of the saga is thick with irony in two additional respects: one group of stakeholders has insisted on extra time to file comments – because they're very busy at the moment – even though catering to their needs aggravates the issue of regulatory uncertainty.[2] Without any evidence of self-awareness, this side also argues that the sale of prioritized network services is a *Very Bad Thing* because, in their analysis, granting favors to one party makes the network less beneficial to others.

Complaints from many commenters about the nature of the Commission's questions are also ironic. Public Knowledge complains that the public notice violates the APA's notice and comment provision:

---

[2] County of Santa Clara and City of Los Angeles, "Initial Comments of the County of Santa Clara, Santa Clara County Central Fire Protection District, and the City of Los Angeles in Response to the Commission's February 19, 2020 Public Notice, Restoring Internet Freedom, WC Docket Nos. 17-108, 17-287, 11-42," April 20, 2020.

> *Under the Administrative Procedure Act (APA), the Commission must provide the opportunity for notice and comment before adopting any rule. As the Supreme Court recently emphasized, "[n]otice and comment gives affected parties fair warning of potential changes in the law and an opportunity to be heard on those changes—and it affords the agency a chance to avoid errors and make a more informed decision." Additionally, the Commission must provide clear notice of its intent so that a reasonably interest party can discern what issues will logically arise from the proceeding. The Commission may not seek to "lull" parties into complacency by camouflaging proposals for major rule revisions as a mere effort to refresh the record.*[3]

So, we are not meant to be concerned about granting the FCC the power to make up regulations on the fly as long as the proceeding that gives them such power is properly noticed. Check.

Internet policy in the United States of America in the year 2020 clearly has deeper problems than the mere regulatory classification of broadband Internet Service. But here we are, once again.

2. Most comments repeat well-worn arguments

Close examination of comments filed by major stakeholders in the initial phase of this comment cycle reveals extraordinarily little in the way of new or unique information. Most parties agree that the Internet is a critical system, more important to Americans than ever before. There is little disagreement on the fact that broadband networks have maintained strong performance while nearly all the rest of the economy has stuttered.

Nearly all comments from the Title II side mention an error committed by a customer service agent at Verizon during the most recent two California wildfires, but none acknowledge that the issue was rectified without FCC intervention. Sadly, even the

[3] Public Knowledge et al., "COMMENTS OF PUBLIC KNOWLEDGE, ACCESS HUMBOLDT, ACCESS NOW, AND NATIONAL HISPANIC MEDIA COALITION," April 20, 2020, p. 4.

FCC lacks the power to eliminate human error. Any regulation aimed at the achievement of human perfection is bound to fail, of course.

Title II enthusiasts uniformly assert that the Commission has failed to ask the proper questions. But they nevertheless go on to offer responses to the questions they would have liked the Commission to ask, such as the general impact of the RIF Order on public safety.[4] In many cases, these criticisms of the public notice's questions reveal that they do, in fact, invite the responses filers would most like to make.

Too many comments in the first round rely entirely on assertions without evidence, such as the prediction that public safety will suffer harms from Title I in the event of a major crisis. As we are currently in such a crisis – and have been since March – surely it should be possible for advocates to produce the goods. The closest the Title II side came in the first round was the speculation offered by EFF on the impact of data caps:

> *People being unable to work or attend school because of data caps was a major concern. However, many ISPs suspended data caps during the crisis, as the caps were artificially imposed for profit purposes, not because they were required to manage the networks.*[5]

But even EFF's source – a somewhat scurrilous blog post – was forced to admit that ISPs had voluntarily suspended data caps, rendering the issue moot.[6] Nonetheless, Free Press pounced on the question of data caps in its version of the California Wildfire affair:

> *Since the harm was caused by a data cap issue rather than discriminatory throttling of a particular source or sender, the 2015 Open Internet Order 's "bright-line" Net Neutrality rules might not apply. But this is not the end of the*

---

[4] *County of Santa Clara and City of Los Angeles, page 4.*

[5] Electronic Frontier Foundation, "COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION," April 20, 2020.

[6] Karl Bode, *Comcast Suspends Data Caps in Wake of Coronavirus,* VICE (Mar. 13, 2020, 3:49 PM), https://www.vice.com/en_us/article/m7qk4n/comcast-suspends-data-caps-in-wake-of-coronavirus

> *conversation, because Title II allowed the Commission to do more than just enforce those Net Neutrality rules. It also empowered the Commission to assess and prevent other forms of unjust or unreasonable behavior – which may well have included Verizon's decision to cap and throttle firefighters during an emergency – as well as the other potential public safety pitfalls and disasters for residential customers consistently raised by state, county, and municipal officials in the Mozilla case and the Commission's RIFO docket. [references omitted]*[7]

As noted, the issue was resolved without any kind of FCC intervention because it was error rather than policy.

Finally, many commenters allege that a fulsome history net neutrality violations exists despite their inability to point to any examples following the 2005 Madison River case. EFF is a good example:

> *Unfortunately, we have evidence that, absent net neutrality protections, [blocking third party voice services] is exactly what [ISPs] will do. In an emergency, Americans need to be able to call emergency services, and it can't matter whether this is a traditional phone call or an Internet-enabled call. We have evidence of ISPs violating net neutrality based on this exact distinction. In 2005, Madison River, a North Carolina ISP, blocked customers from using the "Voice over Internet Protocol" (VoIP) service Vonage. In other words, the Internet provider prevented users from making use of a service that allowed them to make calls over the Internet. From 2007-2009, AT&T prevented Apple from making certain VoIP apps (such as Skype) available on the iPhone, also trying to prevent users from making calls "over-the-top" of its service. In 2009, this pattern was repeated with Google Voice.[references omitted]*[8]

---

[7] Free Press, "COMMENTS OF FREE PRESS," April 20, 2020.

[8] Electronic Frontier Foundation, "COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION," 3.

In reality, AT&T reversed its policy on Skype on its own and never asked Apple to block Google Voice.[9] Apple had its own concerns about the security defects in Google's products, as well as other issues with Android.[10]

3. Public Safety Demands Tailored Services

Santa Clara and Los Angeles maintain that ISPs cannot tailor services provided to public safety because it cannot recognize them by source or destination:

> *Put simply, public safety-related communications cannot be identified and treated differently because 21st Century public safety systems rely on myriad connections between and among public officials, members of the public, and public and private systems and platforms.*
>
> *Nor can transmissions from public safety officials reliably be isolated and identified as governmental communications. Increasingly, to reach residents, public safety officials use nongovernmental internet platforms. These uses include not only live-streaming on social media platforms of crucial updates on the COVID-19 pandemic by public health and emergency response officials, as we discuss below, but also posting video or photos of a suspect on Twitter or other social media platforms to engage the public in identifying and apprehending suspects.*[11]

This comment is odd. It puts the fundamental basis of all net neutrality regulations in doubt by rendering them unenforceable. If ISPs cannot discriminate for or against Internet communications on the basis of source and destination, what value can

---

[9] Saul Hansell, "AT&T Reverses Policy on IPhone Internet Calls," *The New York Times*, October 6, 2009, sec. Technology, https://www.nytimes.com/2009/10/07/technology/companies/07phone.html.

[10] "Apple Tells FCC It Didn't Exactly Block Google Voice," *NBC Bay Area* (blog), accessed May 20, 2020, https://www.nbcbayarea.com/news/local/apple-tells-fcc-it-didnt-exactly-block-google-voice/1856497/.

[11] County of Santa Clara and City of Los Angeles, "Initial Comments of the County of Santa Clara, Santa Clara County Central Fire Protection District, and the City of Los Angeles in Response to the Commission's February 19, 2020 Public Notice, Restoring Internet Freedom, WC Docket Nos. 17-108, 17-287, 11-42," 5.

regulations regulating such discrimination possibly have? ISPs cannot discriminate and the FCC cannot enforce if this is true.

As I said in initial comments, one of the benefits paid prioritization would have for both users and suppliers of bespoke Internet service would come from identifying not only requested services but also the requestors of such services. By entering into an agreement with an ISP, users might commit to means by which they can be identified by their service providers. Satisfying the commitment end-to-end requires ISPs to share the agreement with the services with which they interconnect, so the agreement becomes transitive. Making end-to-end agreements is difficult, but not impossible because every interconnection takes place according to an agreement of some kind.

AT&T and Comcast are not automatically interconnected simply because they exist; they agree to interconnect at certain locations at certain capacities by mutual consent. The same goes for the interconnections between ISPs and the services provided by Twitter, by Google as the owner of YouTube, by Microsoft as the owner of Skype, and by Cloudflare and Akamai as hosts of content created by their customers. The Internet may look like the Wild West to lawyers drafting comments with the FCC, but it's quite orderly in practice.

If the concept of "paid prioritization" means anything at all, it requires service providers to know who communicates with them and how their customers' communications are to be treated. In cases where public safety relies on consumer-grade services such as Twitter and YouTube, it is difficult to imagine scenarios in which an ISP would guarantee delivery quality. There is no need for net neutrality regulations to spell this out because the issue in question is simply a false and deceptive offer of service.

Where public safety relies on consumer-grade services to meet its needs, it must be satisfied that the needs so met are no different from those of the ordinary consumer. In order to obtain customized services, public safety needs to meet service providers halfway by choosing an appropriate service level. This is why FirstNet exists: to provide public safety with high reliability, tailored services appropriate to its role in critical events.

The issue underlying Santa Clara's and Los Angeles' confusion is the relative absence of paid prioritization agreements on the consumer Internet. While FirstNet provides crisis-grade management, the consumer Internet does not, largely because of regulatory uncertainty drive by misconceptions about the interaction between consumers and service providers. If public safety wants specialized treatment for its YouTube streams as well as its FirstNet streams, paid prioritization needs to be lawful and available across the entire Internet. Hence, ISPs must remain under Title I for Santa Clara and Los Angeles to get what they say they want.

4. The Discredited Claim that Quality of Service is a Zero-Sum Game

In my initial comments, I alluded to a fundamental misconception that has colored all of the FCC's proceedings on broadband Internet service in this century:

> *Title II proponents mistakenly believe that QoS is a zero-sum game, one in which it is impossible to tailor the management of network resources to the needs of specific organizations and applications without impairing those not so managed. The imagination that can conceive of scenarios in which this is the case can also find the more abundant scenarios in which it is not.*[12]

This error is on display in comments filed by Santa Clara County and the City of Los Angeles, EFF, Free Press, Jon M. Peha and others. Peha's comments are most coherent, but still disappointing in their lack of technical depth.[13]

Peha was FCC Chief Technologist when Kevin Martin chaired the Commission. He has a very impressive resume, which he shares in his comments. Peha was cited in the DC Circuit Court's opinion in Mozilla v. FCC for characterizing the Domain Name Service in a manner largely consistent with my own:

> *Petitioners' amici assert in the context of functional integration (an issue to which we turn in Part I.C.4) that broadband Internet access is not functionally*

---

[12] Richard Bennett, "Comments of Richard Bennett" (High Tech Forum, April 8, 2020).

[13] Jon M. Peha, "The Impact of 'Prioritization' and How the FCC's Order Undermines Public Safety," April 20, 2020.

*integrated with DNS because broadband access works perfectly well without DNS. "Internet architects deliberately created DNS to be entirely independent from the IP packet transfer function," Jordan/Peha Amicus Br. 17, and "a BIAS provider's DNS is an extraneous capability * * * not required for the core service," id. at 17–18 (emphasis added). But if DNS is "extraneous" to operating the network, it is at least debatable whether DNS is used in "the management, control, or operation of a telecommunications system or the management of a telecommunications service." Amici for the Commission make related points, observing that "[a]n app's DNS translation transaction ends before the BIAS transmission begins," "DNS transactions do not provide the BIAS provider with information about the best path to the destination," and they "do not have the power to either optimize or impair the BIAS provider network." Bennett et al., Amicus Br. 13. Thus it is at least reasonable not to view DNS as a network management tool. Id. at 13–14. Granted, Jordan and Peha remark that running DNS helps an ISP "reduce[] the volume of DNS queries passing through its network." Jordan/Peha Amicus Br. 18. But in the deferential posture of Chevron the points quoted above by Jordan/Peha seem in part to support the Commission's reading of the record (consistent with Bennett et al.) as showing that, whereas "little or nothing in the DNS look-up process is designed to help an ISP 'manage' its network," 2018 Order ¶ 36, DNS is "essential to providing Internet access for the ordinary consumer," id., for whom "DNS is a must," id. ¶ 34 (quoting Brand X, 545 U.S. at 999).*[14]

Unfortunately, our views diverge in this proceeding.

First, Peha explains prioritization in metaphorical terms:

By definition, it is not possible to give one group higher priority without giving another lower priority. Sometimes airlines overbook a flight, i.e. there are more tickets sold than seats on the plane. When deciding which ticket-holders to

[14] Mozilla Corp. v. FCC, No. 940 F.3d 1 (D.C. Circuit October 1, 2019).

allow on the plane, some airlines prioritize frequent flyers. Prioritizing frequent flyers necessarily increases the number of non-frequent-flyers who miss their flight.[15]

The more relevant parallel in relation to air travel is the boarding lane system. Every ticketed traveler will be boarded, and every traveler will reach the destination airport at the same time, but the time spent waiting to board will vary by class of service and other factors. Boarding lanes do not cause anyone to miss their flight, but they do allow active duty military and families with small children to spend less time in the boarding area. Most regard this is as good thing.

Peha quickly asserts that prioritization decisions have deep impact by necessarily degrading service for all non-priority applications:

Indeed, with most forms of differential treatment in the Internet that contend with resource constraints, improving some measure of performance such as latency for one class of traffic usually means degrading that same measure of performance for other traffic.[16]

This gloss misses the fact that Internet prioritization is simply a question of moving individual packets from one position in a queue to another. Whether this activity has an impact on a given application – and whether its impact is perceptible – depends on the nature of the application and the state of the network. Assume that one passenger in a boarding lane is in the middle of a family. Moving that passenger ahead of the family will not affect the family's access to the airplane because the family is not fully boarded until the last member takes their seat. Where the solo traveler is an isolated voice packet generated by a VoIP app and the family is a clump of Netflix packets, the VoIP packet's queue position is immaterial. The last member of the family takes their seat at the same time regardless of when the solo traveler enters the jetway.

This example shows that no single metric of transmission quality is equally meaningful for all applications. We can borrow from one application to improve another without materially affecting most applications.

---

[15] Peha, "The Impact of 'Prioritization' and How the FCC's Order Undermines Public Safety."

[16] Peha.

Peha then goes on to lose the distinction between brief delays due to de-prioritization and long ones:

> *While it is true that there is some traffic for which even very large delays are not particularly harmful, this is not true for the majority of traffic on the Internet today. AT&T cites web browsers as an example of an application that can tolerate long delays. It is true that browsers can tolerate more delay than VOIP, but a one-second delay would still be very annoying to users, and would constitute harm to both Internet users and to content providers. The fact that some of the applications can tolerate some level of delay does not imply that no amount of delay is harmful.*[17]

The act of prioritizing a single packet by moving it to the head of a transmission queue cannot cause enough delay to affect any Internet application in a noticeable way. This must be the case because the Internet shares circuits, spectrum and other transmission media by design. As I said in my initial comment:

> *The Internet mixes traffic streams on shared communications facilities ("pipes"). Every stream affects every other stream at a microscopic level because each pipe can only carry one message ("packet") at a time. Hence, every packet can potentially delay the packet behind it simply by existing, occupying the pipe for a fraction of a second, and relegating the follower to a transmission queue for a fraction of a second. This is the case whether the network actively manages traffic or not; it's a consequence of sharing a pipe.*[18]

Applications cannot be so sensitive to delay that they fail every time one of their packets enters a transmission queue behind another packet. This defeats the purpose of designing a network around shared transmission facilities and raises the price of the entire system to impractical heights.

While Peha never quantifies "long delays", he seems to imagine scenarios in which one application occupies the transmission queue in some shared switch or router for a second or more. Quality of Service decisions are made in units of milliseconds and

---

[17] Peha.

[18] Bennett, "Comments of Richard Bennett."

microseconds, so the scale of time Peha imagines is ridiculous. Moreover, real-time applications such as Skype and Zoom do not and cannot present large bunches of packets back-to-back the way video streaming apps such as Netflix do. Groups of VoIP packets do not arrive at cable modems together because there are natural gaps between them. After one VoIP packet is transmitted, the VoIP application collects sound for 50 to 100 milliseconds to create the next packet. What takes place in the Internet during that interval is of no interest to the app.

Peha thus makes two common errors in his characterization of prioritization: First, he doesn't properly credit the fact that a single packet causes the same amount of overall delay to a group of data packets from a browser or a video entertainment system whether it is moved to the head of a transmission queue or not. The mere fact that two applications are using a common switch at the same time means there will be some microscopic delay.

Second, Peha fails to distinguish short delays caused by one, two, or even three packets moving around in a queue from the longer (but still fractions of seconds) delays caused by video services bundling up packets in clumps to conserve storage access delays. The latter phenomenon – clumping – is the prime motivator for prioritizing real-time data over entertainment.

One good – if somewhat dated – paper on the way video streaming impacts the Internet is *Application Flow Control in YouTube Video Streams* by Alcock and Nelson.[19] The abstract of the paper follows:

> *This paper presents the results of an investigation into the application flow control technique utilised by YouTube. We reveal and describe the basic properties of YouTube application flow control, which we term block sending, and show that it is widely used by YouTube servers. We also examine how the block sending algorithm interacts with the flow control provided by TCP and reveal that the block sending*

[19] Shane Alcock and Richard Nelson, "Application Flow Control in YouTube Video Streams," *ACM SIGCOMM Computer Communication Review* 41, no. 2 (April 15, 2011): 24, https://doi.org/10.1145/1971162.1971166.

approach was responsible for over 40% of packet loss events in YouTube flows in a residential DSL dataset and the retransmission of over 1% of all YouTube data sent after the application flow control began. We conclude by suggesting that changing YouTube block sending to be less bursty would improve the performance and reduce the bandwidth usage of YouTube video streams.

YouTube has taken the advice the authors, but Netflix has not.

Consequently, Peha has destroyed a network management strawman of his own design, while failing to address real uses and potential abuses of practical prioritization schemes.

5. Conclusion

In this remand proceeding, critics of the RIF Order have failed to provide useful or informative insights on ensuring the needs of public safety are protected though regulation. Overall, the impression that light-touch regulation of the Internet provides the best blend of technical progress and protection of legacy Internet applications is reinforced even by critics of the current regime.

Perhaps the long and painful march out of the net neutrality swamp is gathering steam.