April 8, 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

Introduction

I[1] am delighted to offer these 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.

Comments

1. The RIF Order Has No Direct Effect on Public Safety

The FCC's 2017 Report and Order on *Restoring Internet Freedom* (RIF Order) erased the 2015 Report and Order on *Protecting and Promoting the Open Internet* (Title II Order) from the book of FCC regulations over Internet Service.

The principal provision of the Title II Order was a ban on the sale of services that have the effect of "unreasonably [interfering] with or unreasonably [disadvantaging] (i) end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users."[2]

The Title II Order exempted public safety communications from this rule, which only applied to broadband services sold to the general public: "We…reiterate today that our rules are not intended to expand or contract broadband providers' rights or obligations with respect to other laws or safety and security considerations—including the needs of emergency communications and law enforcement, public safety, and national security authorities."[3]

Hence, the RIF Order had no effect on the range of capabilities that service providers may lawfully offer to public safety organizations.

2. The RIF Order Made Public Safety-like Services Broadly Available

Nevertheless, opponents of the RIF Order argued that making "paid prioritization" services available to the general public and to edge providers is *prima facie* unreasonable interference with the free flow of information across the Internet: "Santa Clara County, for example, explained that the 2018 [sic] Order would have a

[2] Title II Order at para 21.
[3] Title II Order at para 299.

"profound negative impact on public welfare, health, and safety" communications. J.A. 3332."[4]

The Court accepted this reasoning as legitimate and declared the RIF Order's lack of explicit language reaffirming the acceptability of offering paid prioritization to public safety while also allowing this vital service to the general public made the RIF Order "arbitrary and capricious."[5]

To reiterate: while the Title II Order permitted the offer of paid prioritization to public safety alone, the RIF Order allowed it to be offered to all, including the public itself.

Predictions of harm to public safety on account of this broader offering have not been realized because they're based on a fundamental misunderstanding of Quality of Service [QoS] provisions generally and of prioritization in particular.

3. Opponents of the RIF Order Misunderstand Quality of Service

It is not necessary for the FCC to include a section with the title "Impact on Public Safety" in every regulation it issues on broadband Internet service. The Commission's charge to consider the needs of public safety can be satisfied by a broader analysis of the technical issues in question as evidenced by the totality of the regulation. The RIF Order includes such analysis.

Nevertheless, the Commission has been ordered to clarify its reasoning on the impact of broadening the market for paid prioritization. As misunderstanding of network QoS is at the root the mistaken push for Title II regulation in a market where it is clearly inappropriate, it is necessary to once again offer a tutorial on the nature of QoS and the ways in which this tool can be used appropriately and inappropriately.

---

[4] *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019), at 94.
[5] *ibid*

4. Quality of Service Is Not a Zero-Sum Game

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.

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.

Unlike legacy networks such as telegraph and telephone, broadband Internet service supports a wide range of applications with different needs. Real-time Internet applications such as VoIP transmit small amounts of information that need to be delivered with minimal latency, while video streaming transmits large amounts of delay-tolerant information.

Video streaming can retransmit lost packets without the user noticing, but VoIP cannot. Managing a multi-purpose network according to Quality of Experience [QoE] maximizes opportunities for free and effective speech. This is permitted under the RIF Order but not (fully) permitted under the Title II Order.

5. Quality of Service by Contract is Broadly Beneficial

Most of the traffic that transits the Internet today is encrypted, hence traditional tools for recognizing traffic streams in order to divine their service needs are less effective than they once were. Hence, other forms of traffic analysis and other commercial relationships are necessary for active traffic management to be successful.

The principal means by which public safety's needs to met today is FirstNet, a network that prioritizes the needs of public safety over those of the general public by network segregation and by active management. FirstNet is exempt from FCC regulations

on broadband Internet services. In addition to FirstNet, public safety organizations may buy services in the commercial marketplace tailored to general business that are also exempt from FCC regulation.

Thirdly, public safety may purchase the same services sold to the general public. In the third case, providers generally relax account restrictions during times of crisis, effectively providing high quality commercial service for the price of generic consumer service. This promotion depends on human intervention and is not always perfect. The infamous California wildfires in October 2017 (the Tubbs Fire, when Title II regulation was in effect) and November 2018 (the Camp Fire, when it was not) were both accompanied by specific failures to promote generic plans, for example. Both incidents were resolved as human errors.

"Paid prioritization" (more accurately, "QoS by contract") is a means of triggering active management of network traffic without the pitfalls of direct human intervention. Making this service available to both public safety actors and the public itself makes the public safer by eliminating a source of error.

6. Fuller Information About Quality of Service

For a more complete explanation of network QoS, the Commission should review the BITAG report, *Differentiated Treatment of Internet Traffic*.[6] In particular, I recommend Section 2, "Differentiation in IP networks", Section 5.1, "Interactive service differentiation". Observation 6.4, "Differentiated treatment can produce a net gain in Quality of Experience (QoE)", explains the central issue:

> *As introduced in the Section 2 discussion on the relationship between QoS and QoE and later in Section 5.1, when differentiated treatment is applied with an awareness of the requirements for different types of traffic, it becomes possible to create a benefit without an offsetting loss. For example, some differentiation techniques improve the Quality of Service (QoS) or Quality of Experience (QoE) for*

[6] Broadband Internet Technical Advisory Group, *Differentiated Treatment of Internet Traffic*, October 2015, Boulder, Colorado, https://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf

particular applications or classes of applications without negatively impacting the QoE for other applications or classes of applications. The use and development of these techniques has value."

Similarly, the April 17, 2018 hearing of the House of Representatives Communication and Technology Subcommittee, "From Core to Edge: Perspective on Internet Prioritization" cast considerable light on the value of selective prioritization.[7] Witness testimony for this hearing casts further light on the productive use of QoS for contract. In particular, I recommend my comments on the use of QoS by contract to replace costly private lines with less expensive Internet pipes: "A recent Gartner Group report identifies 16 of more than 40 firms offering [managed network services]. Their general value proposition lies in allowing customers to save money by using the Internet as a substitute for Business Data Services or private lines. Gartner reports that SD-WANs may be deployed by organizations on a "DIY" basis as ITXC did; but they may also be offered by network service providers, system integrators, or specialized Managed Service Providers."[8]

7. Objections to the RIF Order Couched in Public Safety Terms Have Been Overtaken by Events

Finally, the opposition to the RIF Order claims that public safety communications with the public are harmed by permitting website operators to "accelerate" their traffic by paying fees to ISPs if public safety does not or cannot afford to pay such fees.

---

[7] House of Representatives Subcommittee on Communications and Technology hearing, "From Core to Edge: Perspective on Internet Prioritization", April 17, 2018, Washington DC, https://energycommerce.house.gov/committee-activity/hearings/hearing-on-from-core-to-edge-perspective-on-internet-prioritization.

[8] Richard Bennett, testimony before House of Representatives Subcommittee on Communications and Technology hearing, "From Core to Edge: Perspective on Internet Prioritization", April 17, 2018, Washington DC, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Bennett-CAT-Hrg-on-From-Core-to-Edge-Perspective-on-Internet-Prioritization-2018-04-17.pdf

The California Public Utility Commission (CPUC) predicted that the RIF Order would: ""profoundly impair[]" the ability of state and local governments "to provide comprehensive, timely information to the public in a crisis."[9]

Law professor and one-time CPUC Commissioner Catherine Sandoval predicted that the RIF Order would prevent public power companies from requesting demand reductions from customers by disabling: "…Internet-based "demand response programs" that are "activated during times of high demand, or when fire or other emergencies make conservation urgent," and "call on people and connected devices to save power."

The California Department of Forestry and Fire Protection (CDFFP) pleaded that it "depends on broadband access, speed, and reliability" in order to "track fire threats, fires, and manage forests and vegetation" to prevent fires", a capability that it apparently believed would cease to exist without the Title II Order's ban on QoS by contract.

These apocalyptic visions of utter catastrophe have not come to pass because they were patently hyperbolic from the outset. In response to the COVID-19 pandemic, we're now conducting a nationwide and worldwide test of the Internet's capacity to function in a public safety emergency that forces the Internet to carry 25 – 50% more traffic (and even more in some cases) than it routinely does. The public health systems at the federal, state, and local level are continuing to function without notable incident. Every day the White House coronavirus task force streams a briefing to the public through Facebook and several news websites despite efforts by some to censor these communications.

Social media platforms and networks are awash with commentary on the pandemic, both true and false. Millions of Americans are working, schooling, and assembling virtually through Virtual Private Networks, video conferencing platforms, and webcasting. While some users experience slowdowns in their self-managed Wi-Fi networks, it's fair to say that no one is unable to communicate on account of their inability to pay QoS fees.[10]

---

[9] DC Circuit opinion at 95.

[10] Aldo Svaldi, "Comcast Experiencing Much Heavier Internet Traffic, but No Traffic Jams," *Denver Post*, March 31, 2020, https://www.denverpost.com/2020/03/31/coronavirus-colorado-comcast-traffic-heavy-no-slowing/.

The present state of the Internet amid the pandemic is ample evidence that the prophecies of doom shamelessly concocted to induce the DC Circuit to make a poor decision last October are groundless.

The pandemic certainly has illustrated shortcomings in the operation of edge services that are under-provisioned or don't respect privacy. And it has disclosed the fact that those who have Internet service in their homes are strongly advantaged over those who do not. [11] These shortcomings are not related in any way to the RIF Order.

8. Leveling the Public Safety Playing Field

Critics of the RIF Order and advocates of Title II regulation frequently express fears that ISPs harbor secret plans to speed up some websites (and potentially other services) at the expense of others for a fee; this is expressed as selling "fast lanes" and "slow lanes." These fears are expressed in the comments cited above by Santa Clara County, CPUC, Professor Sandoval, and CDFFP in response to the experience of some firefighters during the 2017 and 2018 California wildfires.

While we can sympathize with dedicated public servants doing their best to serve the public in times of crisis, we owe it to them – and to the public they serve – to correct their misunderstandings as best we can. To the extent that American ISPs have ever provided QoS by contract, they have done so in a manner that does not degrade or impair standard Internet service. The FCC's 2010 and 2015 Open Internet Orders permitted the sale of *specialized services* (2010 Order) or *non-BIAS data services* (2015 Order). These services were permitted over pipes shared with standard Internet service as long as they were discernably separate from standard Internet service.

The two orders took different approaches to characterizing these exempt services with respect to presumptions and ways to distinguish them from ordinary consumer-oriented broadband Internet service. Neither order was entirely successful in formulating a clear and unambiguous separation, ultimately arriving at the "I know it when I see it" approach. Such an open-ended regulatory framework for an important aspect of

[11] Richard Bennett, "Broadband in the Lockdown Era," *High Tech Forum* (blog), accessed April 7, 2020, https://hightechforum.org/broadband-in-the-lockdown-era/.

commerce is unsatisfactory because it prevents firms from knowing *ex ante* if a given service offering is acceptable. Sellers of specialized services were thus required to play regulatory roulette instead of serving the people.

Perhaps ironically, FirstNet and other broadband plans used by public safety rightly belong under the umbrella of specialized services, critical to the public safety mission. Other broadband services used by public safety are clearly outside the specialized services realm – public-facing websites for example – and others are hard to classify.

Is a personal cell phone service used by a firefighter both on and off the job a public safety service? Complaints about data caps raised during the Tubbs Fire and the Camp Fire suggest that fire protection organizations want consumer plans to be treated as specialized services on special occasions. Whether it's reasonable for ISPs to discriminate by the occupations of their customers is an interesting question, the answer to which would have implications for regulatory reasoning around public safety networking.

Whether QoS by contract is segregated from best-efforts consumer broadband or integrated within its regulatory umbrella, the attention paid to this service in every FCC Open/Free Internet order since 2010 suggests it's an important feature to have. As long as ISPs are accountable to be truthful with respect to their claims about the range of sites and services customers can reach and the speeds they can expect, I don't regard the risk of QoS degrading best-efforts services to be substantial.

The virtue of making QoS by contract available to both the public and the public safety community – as the RIF Order does – is the recognition that the public has a complementary role to play in ensuring their own safety. We recognize the public's role in reducing the spread of SARS-CoV-2, but we didn't all see it with respect in the California wildfires. The RIF Order put the public and the public safety community on a level playing field, empowering each to protect public safety in its unique way.

Conclusion

QoS by contract has value for the business community and the public safety community because it improves the overall efficiency of the Internet, enables it to support a wider range of applications, reduces costs, and empowers users to control their own resources. The RIF Order did not take any of these benefits away, it simply extended them to the entire public, including off-duty firefighters. This is such a self-evident win for public safety that it hardly needs explaining.