OFFICE OF THE COUNTY COUNSEL
COUNTY OF SANTA CLARA

County Government Center
70 West Hedding Street
East Wing, 9th Floor
San José, California 95110-1770

(408) 299-5900
(408) 292-7240 (FAX)

James R. Williams
COUNTY COUNSEL

Greta S. Hansen
CHIEF ASSISTANT COUNTY COUNSEL

Robert M. Coelho
Tony LoPresti
Steve Mitra
Kavita Narayan
Douglas M. Press
Gita C. Suraj
ASSISTANT COUNTY COUNSEL

February 8, 2021

ELECTRONICALLY SUBMITTED (https://www.fcc.gov/ecfs)

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th St. SW
Washington, DC 20554

Re: Petition for Reconsideration of the County of Santa Clara and Santa Clara County Central Fire Protection District of the Order on Remand, DA FCC-20-151
Restoring Internet Freedom, WC Docket Nos. 17-108, 17-287, 11-42

Dear Secretary Dortch:

Enclosed please find the County of Santa Clara's and Santa Clara County Central Fire Protection District's petition for reconsideration of the Commission's *Order on Remand* in the Restoring Internet Freedom and Lifeline proceedings, DA FCC-20-151, WC Docket Nos. 17-108, 17-287, 11-42.

Very truly yours,

JAMES R. WILLIAMS
County Counsel

/s/ Raphael N. Rajendra

Raphael N. Rajendra
Deputy County Counsel

Meredith Johnson
Deputy County Counsel

Phillip R. Malone
Juelsgaard IP and Innovation Clinic
Mills Legal Clinic at Stanford Law School

Jef Pearlman
Intellectual Property &
Technology Law Clinic
USC Gould School of Law

Before the
Federal Communications Commission
Washington, DC 20554

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

PETITION FOR RECONSIDERATION OF THE COUNTY OF SANTA CLARA AND THE SANTA CLARA COUNTY CENTRAL FIRE PROTECTION DISTRICT

JAMES R. WILLIAMS
County Counsel
County of Santa Clara
70 West Hedding Street
East Wing, 9th Floor
San José, CA 95110
(408) 299-5900

February 8, 2021

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, DC 20554

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

PETITION FOR RECONSIDERATION OF THE COUNTY OF SANTA CLARA AND THE SANTA CLARA COUNTY CENTRAL FIRE PROTECTION DISTRICT

Pursuant to FCC Rule 1.429, the County of Santa Clara (the "County") and the Santa Clara County Central Fire Protection District ("County Fire"), by their undersigned counsel, hereby respectfully request that the Federal Communications Commission (the "Commission" or "FCC") reconsider its *Order on Remand* in the Restoring Internet Freedom and Lifeline proceedings.[1] The *Order on Remand* purports to respond to *Mozilla Corp. v. FCC*,[2] in which the D.C. Circuit held in pertinent part that the FCC's *Restoring Internet Freedom Order* (the "*2018 Order*")[3] was arbitrary and capricious because the Commission abjectly failed to consider the impact of the *2018 Order* on public safety.[4] But the *Order on Remand* fails to grapple with the serious risks to life and property occasioned by the *2018 Order*; wrongly suggests that the *ex post* remedies available under the *2018 Order* are an adequate substitute for the *ex ante* conduct rules applicable under the Commission's prior orders; and abdicates the FCC's regulatory

[1] *Order on Remand*, DA FCC-20-151, WC Docket Nos. 17-108, 17-287, 11-42 (rel. Oct. 29, 2020) (the "*Order on Remand*"), subsequently published as a final rule in synopsis form at *Restoring Internet Freedom; Bridging the Digital Divide for Low-Income Consumers; Lifeline and Link Up Reform and Modernization*, 86 Fed. Reg. 994 (Jan. 7, 2021).

[2] *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019).

[3] *Restoring Internet Freedom*, 33 FCC Rcd. 311 (2018) ("*2018 Order*").

[4] *Mozilla*, 940 F.3d at 62-63.

responsibility in favor of the wholly speculative assertion that individual corporate actors in an unregulated market will forgo revenue opportunities in favor of self-imposed restrictions that serve the collective good. Its analysis is superficial, does not adequately respond to the remand in *Mozilla*, does not protect public safety, and must be reconsidered.

We urge that, upon further and more careful consideration of the public safety implications of the *2018 Order*, the Commission should conclude:

(1) the *2018 Order*'s repeal of mandatory open internet conduct rules and disclaimer of authority to oversee and impose conduct requirements on Internet service providers (ISPs) offering broadband Internet access service (BIAS) poses unacceptable and unnecessary risks to public safety; and

(2) those risks to public safety gravely outweigh the *Order on Remand*'s unsubstantiated guesswork that unregulated markets will generate expanded, upgraded, and more robust Internet infrastructure, as well as corporate policies that adequately protect consumer access to the Internet and the content providers through which they make use of that Internet access.

Accordingly, the Commission should reverse or vacate the *Order on Remand*, vacate the *2018 Order*, and revert to the mandatory open internet conduct rules set out in the Commission's 2015 *Title II Order*[5] ("Net Neutrality Rules") while the Commission considers what modifications to the *Title II Order*, if any, would further advance its duty to protect the public. To the extent the Commission determines necessary, the Commission can conduct a rulemaking to further expand the record upon which it makes its decision.

I. INTRODUCTION AND SUMMARY

The Commission's decisions "must take into account its duty to protect the public."[6] That was clear before *Mozilla*, it was clear throughout the remand proceedings, and it is clear now.

[5] *In re Protecting and Promoting the Open Internet*, GN No. 14-28, DA FCC-15-24, 80 Fed. Reg. 19738 (Apr. 13, 2015) (the "*Title II Order*").

[6] *Mozilla*, 940 F.3d at 60 (quoting *Nuvio Corp. v. FCC*, 473 F.3d 302, 307 (D.C. Cir. 2006)) (internal quotation marks omitted).

This is so because "the Commission is required to consider public safety by its enabling act."[7] Indeed, the Communications Act states plainly that the Commission exists "for the purpose of, among other things, 'promoting safety of life and property through the use of wire and radio communications.'"[8] The Commission's duty is particularly important when it exercises its "responsibility to regulate" the telecommunications market, which Congress "has repeatedly deemed important to protecting public safety."[9]

Despite that clear mandate, the Commission wholly failed to consider public safety in the *2018 Order*. In doing so, the D.C. Circuit explained, the Commission had "entirely" missed the fact that, "whenever public safety is involved, lives are at stake. . . . [T]he harms from blocking and throttling during a public safety emergency are irreparable. People could be injured or die."[10] While the *Order on Remand* pays lip service to this fact and repeatedly mentions the phrase "public safety," it fails to actually consider what "public safety" communications look like in the 21st century, to account for the reality that "lives are at stake" when public safety operations are hampered, and to acknowledge that public safety harms are irreparable once they occur.

The *Order on Remand*'s analytical failures are unsurprising because it rests, first and foremost, on the false premises that it is possible *ex ante* to identify communications that are essential to public safety and to treat them differently from other communications, and that even if mass-market BIAS plans do not provide consumers with unfettered Internet access, public safety is adequately protected by other communications channels. From the outset, the Commission's Public Notice opening the record on remand misframed the inquiry. As the County, County Fire, and City of Los Angeles explained in their April 20, 2020 comment, "The question before the Commission after *Mozilla* is how public safety is affected—and, vitally, whether and how the connections between public safety officials and the public are threatened—

[7] *Id.* at 59-60 (quoting *Nuvio*, 473 F.3d at 307) (internal quotation marks and alterations omitted).
[8] *Id.* (quoting 47 U.S.C. § 151).
[9] *Id.* at 60 (quoting *Nuvio*, 473 F.3d at 307).
[10] *Id.* at 62.

by the [*2018*] *Order*'s repeal of the Net Neutrality Rules. But the Commission sidesteps that question in favor of narrower and misdirected inquiries."[11]

This fundamental failure infected every component of the *Order on Remand*'s response to the public safety remand. Specifically, the *Order on Remand* dismisses the public safety harms extensively described in the record and articulated in *Mozilla* and re-endorses the *2018 Order*'s "light-touch regulatory approach." It justifies its re-endorsement of that approach by concluding that (1) the approach is not "likely to adversely impact public safety," and (2) "even if there were some adverse impacts on public safety applications in particular cases—which we do not anticipate—the overwhelming benefits of Title I classification would still outweigh any potential harms."[12]

Based on the evidence in the record before the Commission, as well as more recent developments, the *Order on Remand*'s analysis is flatly incorrect. The Commission cannot fulfill its duty to protect public safety without robust *ex ante* conduct rules under Title II, and the *Order on Remand* is wrong, as a matter of evidence and logic, to insist that public safety will be adequately ensured by the corporate behavior the *2018 Order* baselessly predicted would occur in in an unregulated BIAS market.

II. THE COMMISSION CANNOT FULFILL ITS DUTY TO PROTECT PUBLIC SAFETY WITHOUT ROBUST *EX ANTE* CONDUCT RULES UNDER TITLE II

A. In the Internet Age, The Protection of Public Safety Requires That Community Residents Have Robust and Unfettered Access to the Internet

To fulfill their missions, public safety agencies must effectively and efficiently communicate to, and receive information from, the residents they serve and protect. These agencies increasingly do this over the Internet. Accordingly, they must be able to communicate to residents without regard to the ISPs through which those residents access the Internet or the

[11] 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) ("Santa Clara & Los Angeles April 20, 2020 Comment"), at 4, incorporated herein by reference and available at https://www.fcc.gov/ecfs/filing/10421077992221 and https://perma.cc/SH6S-3UKB.

[12] *Order on Remand* at ¶ 20.

private-sector platforms and edge content providers that enable those communications. It was true three years ago that local governments' "internet-based services depend[ed], in many cases, on *community members*' access to broadband internet on nondiscriminatory terms,"[13] and that is even more true now, both due to the COVID-19 pandemic and because communitywide communication increasingly occurs online.[14]

The *Order on Remand* offers no rejoinder to the core danger the *2018 Order* poses to public safety. As the County previously described that danger:

> 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. Moreover, the [*2018*] *Order* disclaims the Commission's authority to require ISPs to segregate, and prioritize public-safety communications. So even if it were technologically possible to *identify* those communications ahead of time, it is impossible under the [*2018*] *Order* to leverage that technical possibility to protect public safety.[15]

As the COVID-19 pandemic pushes ever more public safety officials, and many other workers, to work from home over mass-market BIAS connections governed by the *2018 Order*, the public-safety risks posed by the Commission's refusal to require ISPs to carry Internet traffic on nondiscriminatory terms pile up. And they are compounded by the Commission's disclaimer of authority to impose discrete rules or requirements for particular circumstances that may arise. Yet these risks are not COVID-specific: well before COVID, "it was entirely predictable—in

[13] County & County Fire's December 6, 2017 *ex parte* submission, WC Docket No. 17-108 (the "Santa Clara December 6, 2017 Comment"), at 2 (emphasis added), incorporated herein by reference and available at https://www.fcc.gov/ecfs/filing/1207942320842 and https://perma.cc/7MMJ-7CWX.

[14] Santa Clara & Los Angeles April 20, 2020 Comment at 4-5.

[15] Santa Clara & Los Angeles April 20, 2020 Comment at 5.

fact, predicted by the [County]—that during a public-health emergency, public safety would rely heavily on robust and unencumbered community access to broadband internet."[16]

The County, County Fire, and City of Los Angeles previously explained that local governments rely heavily on private-sector social media platforms and a wide variety of edge content providers to disseminate *and collect* time-sensitive public safety information—not only for COVID-related orders and information, but also police announcements during active shooter scenarios, adverse weather events, wildfires and other firefighter response, and other emergencies.[17] Likewise, the U.S. Department of Homeland Security explained in a 2013 paper that relevant literature and real-world experience in nine different public safety emergencies made clear that real-time two-way information exchange through social media plays a crucial role in emergency response. It explained: "Through the use of social media, members of the public who witness incidents can provide public safety organizations with timely, geographic-based information. This information can be used by decision-makers in planning response strategies, deploying resources in the field, and, in turn, providing updated and accurate information to the public."[18]

None of the systems or operations that local governments use to manage and respond to emergencies can work if ISPs providing residents (including officials working from home) with BIAS through mass-market plans have blocked, throttled, or otherwise impaired or degraded their access to the platforms on which they can exchange crucial, time-sensitive public safety

[16] Santa Clara & Los Angeles April 20, 2020 Comment at 5.

[17] *See, e.g.*, U.S. National Library of Medicine, Disaster Information Management Research Center, *Social Media Analysis During Disasters* (last updated Feb. 2021), https://perma.cc/C4RE-MXUQ (emphasizing that both public safety agencies and the broader community rely on social media platforms to distribute and gather critical situational awareness information during emergencies); R. Moore & A. Verity, *Hashtag Standards for Emergencies*, United Nations Office for the Coordination of Humanitarian Affairs Policy and Studies Series (Oct. 2014), https://perma.cc/DK38-44W5; J. Bonnan-White et al., *Snow Tweets: Emergency Information Dissemination in a US County During 2014 Winter Storms*, PLoS Currents (Dec. 2014), https://perma.cc/XDU5-6SXK (analyzing public safety agencies' Twitter usage during adverse weather events and emphasizing that such agencies can use social media to disseminate critical real-time information during large events).

[18] U.S. Dep't of Homeland Security, *Innovative Uses of Social Media in Emergency Management* (Sept. 2013), https://perma.cc/WL3B-4JCP.

information with their governments during emergencies. It is no exaggeration to say that when an ISP blocks or deprioritizes residents' access to these platforms, lives are at stake.[19]

To these lived realities of public safety agencies, the *Order on Remand* offers misdirection rather than protection. Its celebration of networks that are dedicated to first responders and not governed by the *2018 Order* is entirely beside the point. This is no criticism of FirstNet, services that ISPs have introduced to compete with it, voice services, traditional 911 networks, and enterprise-grade BIAS with Quality-of-Service guarantees, each of which serves an important purpose and all of which are outside the *2018 Order*'s scope. But local governments protect public safety through means far beyond the first responders who may use these systems. Thus, their existence is irrelevant to the question *Mozilla* directed the Commission to address: whether and to what extent to modify the *2018 Order* itself due to its adverse effects on public safety and the myriad ways that public safety operations rely on mass-market BIAS. Because the outward-facing nature of public safety operations necessarily means public safety agencies rely on unfettered transmission of Internet traffic to and from the public over the mass-market BIAS plans that are subject to the *2018 Order*, the existence of public safety-specific channels like FirstNet are simply not responsive to the D.C. Circuit's remand. Accordingly, the *Order on Remand*'s reliance on these channels[20] is a material error that must be reconsidered.

B. *Ex Ante* Conduct Rules Are Essential to Public Safety Because Irreparable, Often Fatal Harms Can Result When ISPs Throttle or Block Internet Traffic During Public Safety Emergencies

The *Order on Remand* disregards the reality of how public safety communications actually operate, particularly during emergency response. It then makes matters worse by wrongly assuming that after-the-fact remedies can effectively take the place of *ex ante* rules that would prohibit the harmful conduct in the first place. The Commission is flatly incorrect that public safety harms caused by ISP practices prohibited by the *Title II Order* but permitted by the *2018 Order* could be effectively remedied after the fact. Neither money judgments nor

[19] *Mozilla*, 940 F.3d at 62.

[20] *E.g.*, *Order on Remand* at ¶¶ 24, 25, 32, 33, 56, 57, 66.

subsequent ISP promises not to repeat the practice can undo the harm to the public, or lives potentially lost, from communication challenges that first responders have in engaging with the public or each other.

In this respect, the *Order on Remand* not only disregards the record, it also countermands the D.C. Circuit's clear admonition in *Mozilla*. The FCC claimed that despite the repeal of the Net Neutrality Rules, edge providers and consumers would remain protected against ISP abuse by market forces, consumer choice, reputational concerns, and *ex post* remedies available from consumer-protection agencies. The D.C. Circuit forcefully disagreed: the asserted protections were "barely" acceptable *outside* the public safety context, and flatly "too little, too late" in response to public safety concerns.[21] Nonetheless, the *Order on Remand* essentially repeats, without new evidence or analysis, the FCC's litigation position that market forces and *ex post* remedies adequately respond to public safety concerns, as well as to edge providers' and consumers' concerns. Simply restating the FCC's litigation position is contrary to *Mozilla* and unsupported by any reasoning.

1. **Ex Post *Enforcement is An Insufficient Remedy for Public Safety Harms.*** Even outside the public safety context, the D.C. Circuit questioned the Commission's reliance on after-the-fact antitrust and consumer-protection enforcement as a sufficient form of consumer protection, noting that the Commission had "theorized why antitrust and consumer protection law is preferred to *ex ante* regulations" but "failed to provide any meaningful analysis of whether these laws would, in practice, prevent blocking and throttling."[22] As a result, the Commission "barely" survived arbitrary and capricious review on that issue.[23]

In the public safety context, though, there can be no doubt that after-the-fact enforcement via antitrust and consumer-protection laws will not protect the public. In the emergency circumstances described above, harms caused by blocking and throttling are irreparable. For example, such practices could interfere with the communications about the existence of a fire

[21] *Mozilla*, 940 F.3d at 59, 62.

[22] *Mozilla*, 940 F.3d at 59.

[23] *Mozilla*, 940 F.3d at 59.

line or evacuation zone, the location of flooding, or the location of criminal suspects or missing individuals, among many other critical and time-sensitive communications. The harm caused by blocking and throttling these types of communications simply cannot be remedied after the fact, and ISP practices previously barred by the Net Neutrality Rules are impossible for local governments to identify, let alone correct for. As the Court aptly stated, "unlike most harms to edge providers incurred because of discriminatory practices by broadband providers, the harms from blocking and throttling during a public safety emergency are irreparable. People could be injured or die."[24]

This is precisely why the Court held the *2018 Order*'s reliance on market forces and after-the-fact consumer-protection remedies was "too little, too late" in response to public safety concerns: market forces and after-the-fact remedies are a "facially inadequate" response to the record evidence that irreparable, often fatal harms can result from an ISP blocking or throttling Internet traffic during public safety emergencies.[25] Nothing in the *Order on Remand* overcomes these fundamental failings.

2. The Federal Trade Commission Has Never Been an Adequate Substitute for Oversight by the Agency with Telecommunications Expertise. The inadequacy of after-the-fact enforcement for public safety harms is a matter of common sense. But *even if* some form of *ex post* consumer-protection enforcement were theoretically responsive to public safety concerns, the *Order on Remand* places unjustified reliance on "the privacy and consumer protection authority of the Federal Trade Commission over ISPs." The *Order on Remand* notes that the FTC promised the FCC that it "will 'investigate and take enforcement action *as appropriate*'" against ISPs.[26] Likewise, the *2018 Order* itself said that its fundamental determination to abandon the rules set out in the *Title II Order* "is informed—as it must be—by the return of

[24] *Mozilla*, 940 F.3d at 62.

[25] *Mozilla*, 940 F.3d at 62. The Court explained that the FCC's response was "too late" because it was "appellate counsel's *post hoc* rationalization for agency action" rather than a ground on which the FCC based the *2018 Order*. *Id.*

[26] *Order on Remand* at ¶¶ 4, 39 (emphasis added)

jurisdiction to the [FTC] to police ISPs for anticompetitive acts or unfair and deceptive practices."[27]

The fallacy of this argument was apparent before the *2018 Order* issued. But the FCC's reliance on the FTC's supposed authority in its October 2020 *Order on Remand* is even more baffling: after the *2018 Order* issued, the FTC chairman in 2019 specifically disavowed any authority or intention to enforce net neutrality or other open internet rules. He acknowledged that the FTC is not expert in telecommunications matters; warned that the FTC would not view as unfair or anticompetitive any blocking, throttling, or other ISP behavior previously prohibited by the *Title II* Order; and asserted that the FTC would not take action against ISPs without engaging in a fact specific analysis of whether their conduct "harmed competition through raising rivals' costs or excluding competitors."[28] And no ISP has publicly committed not to block, throttle, or engage in paid prioritization *in the future*[29]—making illusory the FTC's authority to prosecute deceptive trade practices and belying the *Order on Remand*'s claim that ISPs have made "commitments to maintain Internet openness" that "are now enforceable by the Federal Trade Commission (FTC), the nation's premier consumer protection agency."[30] None of this was unknown to the FCC: then-Commissioner Rosenworcel warned in her *2018 Order* dissent that "the FTC is not the expert agency for communications. It has authority over unfair and deceptive

---

[27] *2018 Order* at ¶ 208; *see Fed. Trade Comm'n v. AT&T Mobility LLC*, 883 F.3d 848, 863-64 (9th Cir. 2018) (en banc) ("[T]he exemption in Section 5 of the FTC Act—'except . . . common carriers subject to the Acts to regulate commerce'—bars the FTC from regulating 'common carriers' only to the extent that they engage in common-carriage activity. By extension, this interpretation means that the FTC may regulate common carriers' non-common-carriage activities." (construing 15 U.S.C. § 45(a)(2)).

[28] J. Simons, *Prepared Remarks of Chairman Joseph J. Simons, Free State Foundation Speech at Eleventh Annual Telecom Policy Conference* (Mar. 26, 2019), https://perma.cc/7RKQ-SZUP; *see also* K. Bode, *The FTC Makes It Clear It Can't, Won't Protect Net Neutrality*, Vice (Apr. 2, 2019), https://perma.cc/AAS4-TEK9; W. Davis, FTC Unable To Enforce Obama-Era Net Neutrality Rules, Digital News Daily (Apr. 1, 2019), https://perma.cc/P5DP-U7HL; D. Cameron, *The Head of the FTC Just Debunked the FCC's Favorite Excuse for Killing Net Neutrality*, Gizmodo (Mar. 29, 2019), https://gizmodo.com/the-head-of-the-ftc-just-debunked-the-fccs-favorite-exc-1833673468.

[29] Verizon, *Verizon Online Terms of Service* (Jan. 30, 2020), https://perma.cc/R6H7-6RZD (making no commitments in terms of service not to block, throttle, or engage in paid prioritization, and reserving the right to "change, limit, [or] modify . . . the Service or any part of it with or without prior notice if we elect to change the Service or a part thereof."); Comcast, *Comcast Agreement for Residential Services* (Jan. 2021), https://perma.cc/YPW8-FAXX (similar); *see also* Comcast, *Net Neutrality* (accessed Feb. 2, 2021), https://perma.cc/2RXV-3W2W (stating broadly worded corporate policies only in the present tense).

[30] *Order on Remand* at ¶ 39.

practices. But to evade FTC review, all any broadband provider will need to do is add new provisions to the fine print in its terms of service."[31] The *Order on Remand* does not meaningfully consider how these real-world limitations undermine the *2018 Order*'s theoretical reliance on the FTC for *any* ISP abuse, let alone those that risk grave, irreparable harm to life or property.[32]

C. The *Order on Remand* Undermines the Market for Public Safety-Focused Edge Content Providers on Which Public Safety Relies

The *Order on Remand*'s unbridled optimism about ISPs' behavior in an unregulated market also takes too narrow a view of the full Internet ecosystem upon which 21st Century public safety operations rely. For public-safety agencies and first responders—and all users—the Internet's utility is based not *only* on efficient, robust, and nondiscriminatory transmission of data by ISPs, but also on the websites and applications that edge providers create and maintain. After all, BIAS is useless without content: it is the interaction between BIAS and edge providers, not either of them alone, that generates innovation, consumer demand, investment, and increased capabilities. The *Title II Order* ensured an appropriate balance between ISPs and edge content providers so that both could innovate, invest, and expand without ISPs erecting unscalable barriers to entry for new edge providers (in the form of fees to avoid throttling or to enjoy traffic prioritization).

The *2018 Order* upended that balance by instantiating incumbent ISPs to the exclusion of new BIAS providers[33] and permitting those ISPs to favor well-resourced incumbent edge

---

[31] *2018 Order* at 538 (Dissenting Statement of Comm'r Rosenworcel).

[32] Nor, as other commenters have pointed out, does the *2018 Order* or *Order on Remand* square the circle of local ISP monopolies. The reality is that millions of consumers across many areas of the country have no choice between ISPs: only one in their area provides BIAS. So even if it were conceivable (and it is not) that consumers would select among ISPs based on their net neutrality practices when presented with a meaningful choice, it is illogical that the *Order on Remand* would rely on that theoretical possibility to assert that the *2018 Order*'s transparency rules will incentivize net neutrality practices when consumers have *no* choice because their ISP enjoys a local monopoly over BIAS.

[33] While this Petition for Reconsideration does not focus on the "lapse in legal safeguards" over new ISPs' rights to pole attachments on nondiscriminatory terms that the *2018 Order* occasioned and with which the *Order on Remand* does not seriously grapple, *see Mozilla*, 940 F.3d at 108-09, the County and County Fire agree that those aspects of the *Order on Remand* likewise require reversal upon reconsideration. *See, e.g., Petition for Reconsideration of INCOMPAS*, WC Docket Nos. 17-108, 17-287, 11-42, https://perma.cc/543P-22SH (Feb. 4, 2021), at Part III.

providers. The *Order on Remand* affirms that choice, even though public safety agencies rely on small or new edge providers whose Internet traffic could be blocked, throttled, or subjected to deprioritizing in the absence of *ex ante* net neutrality conduct rules.[34] Local governments around the country rely on public safety-focused startup edge providers including Carbyne, a 911 call-handling platform; OpenALPR, a license-plate recognition tool; SOMA Global, a cloud-based platform of public safety tools; Synapse, a threat-detection system for X-rays and CT scans; and First Due, a pre-incident planning and response platform.[35] When those startup edge providers' Internet traffic is blocked, throttle, or deprioritized, public safety suffers.

This lived reality of public safety agencies and first responders is entirely missing from the Commission's analysis. The *Order on Remand* focuses exclusively on ISPs, virtually ignoring the impact of reclassification and elimination of *ex ante* conduct rules on edge providers.[36] For instance, the entire section concluding that the *2018 Order* benefits innovation, investment, and regulatory certainty addresses *only* the effects on ISPs. The Commission points to comments suggesting that the *2018 Order* "encourages robust investment in *broadband networks* and facilities," "reclassification . . . is likely to increase *ISP* investment and output," and these investments are "likely to affect the risk calculus taken *by ISPs*."[37] The *Order on Remand* barely mentions the systems and companies upon which the County and other local governments rely for public safety operations, as detailed in prior comments. The Commission notes just a single time that the County used WebEOC (a web-based Emergency Operations Center) to communicate through mass-market BIAS.[38] But it fails to address the extent to which

[34] To take one example, "New York City's Domain Awareness System collects and analyzes data from sources including thousands of public, private, and commercial surveillance cameras." Santa Clara & Los Angeles April 20, 2020 Comment at 5.

[35] Carbyne, https://carbyne911.com; OpenALPR, https://www.openalpr.com; SOMA Global, https://www.somaglobal.com; Synapse, https://www.synapsetechnology.com; First Due, https://firstduesizeup.com (all last accessed Feb. 8, 2021).

[36] See *Order on Remand* ¶¶ 19-67.

[37] *Order on Remand* ¶ 32 (emphases added); *see also id.* ¶ 33 (effects of increased ISP performance), ¶ 34 (5G upgrades), ¶ 35 (ISP deployment and speed), ¶ 36 (reliability of ISPs during the COVID-19 pandemic).

[38] *Order on Remand* ¶ 27 n.11. WebEOC is designed to be used over any connection, without regard to ISP or network. This permits critical personnel to access the system from their personal devices, from home, or from the field. Discrimination in provision of broadband service could fundamentally disrupt the operation of this system,

reclassification permits ISPs to undermine the deployment and innovation of WebEOC and other edge systems through traffic prioritization fees that only large incumbent edge providers can afford. Because the *Order on Remand* does not consider these direct harms to edge providers, it fails entirely to consider consequences of such harms—including reduced investment, reduced innovation, and fewer capabilities available to public safety agencies—or the ways those harms undermine public safety.

To that same point, the Commission completely ignores the County's reliance on private-sector platforms such as Zoom to conduct public safety meetings or MailChimp to distribute public health information during the pandemic.[39] The *Order on Remand* does not address the harms to public safety that will result if these and similar private services do not pay ISPs to prioritize their traffic if, as the Order on Remand permits, ISPs were to demand such payments. Nor does the *Order on Remand* justify its surmise that reputational concerns will generate corporate behavior that favors net neutrality practices—particularly when it is functionally impossible to trace an unsuccessful communication to an ISP's blocking, throttling, or deprioritizing and because public safety agencies rely on relatively small edge providers for whom degraded Internet traffic flow can have deleterious effects without generating a public outcry.[40]

The *Mozilla* court held that the *2018 Order*'s conclusion that market forces will protect consumers and edge providers in daily life "barely survive[d] arbitrary and capricious review."[41] The Commission's utter failure to consider the effects on public safety resulted in the remand and this proceeding. But in the *Order on Remand*, the Commission continues its failure to properly consider the effects on public safety edge providers, focusing entirely on ISP innovation and repeating the same baseless assertions that the market will take care of the rest.

---

which functions as a virtual emergency operations center. *See* Santa Clara & Los Angeles April 20, 2020 Comment at 6; Santa Clara December 6, 2017 Comment at 6-7.

[39] Santa Clara & Los Angeles April 20, 2020 Comment at 6, 9.

[40] *See id.* at 9 (explaining that the harms are impossible for local governments to identify and that even where available, *ex post* solutions are inadequate).

[41] *Mozilla* at 59.

III. THE *ORDER ON REMAND* RELIES ON UNSUBSTANTIATED AND INCORRECT PREDICTIONS THAT AN UNREGULATED MARKET WILL GENERATE PUBLIC SAFETY-PROTECTIVE CORPORATE BEHAVIOR

To justify its continuing abdication of the Commission's responsibility to consider and protect public safety, the *Order on Remand* celebrates free market forces, asserting that both public safety and the broader public good are advanced by an unregulated market that will encourage ISPs' innovation and investment. But this reasoning simply does not hold up. There is no evidence that the Net Neutrality Rules impeded innovation and investment or that rolling back those rules has increased them. By contrast, there *is* evidence that the roll-back of the Net Neutrality Rules has allowed ISPs to engage in increased blocking and throttling, putting the lie to the Commission's unfounded conclusion that corporations would voluntarily choose to engage in public safety-protective behavior at the expense of their own profits. An unregulated market plainly undermines public safety rather than advancing it, and the *Order on Remand* is wrong to conclude otherwise.

A. There is No Evidence in the Record that an Unregulated Market Increases Innovation or Investment

The *Order on Remand* posits that the *2018 Order* will result in increased innovation and investment, and that these "overwhelming benefits" outweigh any potential harm to public safety. It also asserts that the *2018 Order* offers ISPs "regulatory certainty" in place of the *Title II Order*'s "fog that stifled innovation."[42] But this is a false dichotomy and factually baseless talking point. There is no evidence in the record that ISPs were unable or unwilling to innovate or invest under the *Title II Order*, nor is there any evidence to suggest that there has been a surge in innovation or investment due to adoption of the *2018 Order*. Indeed, both the *Order on Remand* and the *2018 Order* acknowledge that "many factors affect ISPs' investment decisions,"[43] yet both cling to industry's self-serving and factually baseless claims that the *Title*

[42] *Order on Remand* at ¶ 103; *see also id.* ¶¶ 32-36 (repeating claim of "regulatory certainty").

[43] *Order on Remand* at ¶ 32 (citing *2018 Order* at ¶ 92).

II Order chilled investment and innovation.[44] Inexplicably, moreover, the *Order on Remand* relies heavily—nearly exclusively—on this free-market talking point as its fundamental response to the D.C. Circuit's instruction that it consider the *2018 Order*'s impacts on public safety, but at the same time refuses to "reopen or expand on" the *2018 Order*'s "predictions" about investment and innovation.[45]

Had the *Order on Remand* honestly reexamined whether the *2018 Order*'s unsupported assumptions about the market were factually supported, the Commission would have discovered that the great weight of evidence is to the contrary.[46] In fact, a recent study concluded that Net Neutrality Rules simply have had no effect on investments one way or the other,[47] and other studies reveal that ISP investment remained steady before and after the *2018 Order*.[48] Nor did the *2018 Order* achieve regulatory certainty: proposals continue to circulate in Congress that could dramatically shift the statutory ground upon which the current reclassification questions are considered, and in the face of the FCC's retrenchment, several states, including California, have adopted net neutrality laws that govern ISPs' provision of BIAS to tens of millions of consumers.[49]

Accordingly, while increased innovation and investment are desirable, there is simply no evidence to support the *Order on Remand*'s insistence that the *2018 Order*'s repeal of *Title II Order* Net Neutrality Rules made ISPs more likely to invest and innovate. Nor is there evidence that innovation and investment are more likely to occur without net neutrality rules, or that

---

[44] *Order on Remand* at ¶ 32 & n.130 (citing industry comments and then stating that "these comments lend support to our findings in the [*2018 Order*] that 'reclassification of broadband Internet access service from Title II to Title I is likely to increase ISP investment and output.'" (quoting *2018 Order* at ¶ 98)).

[45] *Order on Remand* at ¶ 32 n.131.

[46] *See, e.g.*, Reply Comment of INCOMPAS, WC Docket Nos. 17-108, 17-287, 11-42 (May 20, 2020), at 12-13, available at https://www.fcc.gov/ecfs/filing/10520050916564 and https://perma.cc/2BW8-4MP3; Letter Comment of Free Press, WC Docket Nos. 17-108, 17-287, 11-42 (Oct. 20, 2020), at 4, available at https://www.fcc.gov/ecfs/filing/10210426129857, https://perma.cc/3JL7-N5DD.

[47] *See* Christopher Alex Hooton, *Testing the economics of the net neutrality debate*, Telecommunications Policy (Vol. 44, Issue 5, June 2020), https://perma.cc/TQT6-ARHT.

[48] *See* J. Brodkin, *Ajit Pai says broadband access is soaring—and that he's the one to thank: Pai's FCC takes credit for new broadband, but progress was similar in Obama era*, Ars Technica (Feb. 20, 2019), https://perma.cc/9PM9-28JC;

[49] *See, e.g.*, California Internet Consumer Protection and Net Neutrality Act of 2018, Cal. Civ. Code §§ 3100-3104.

investment and innovation cannot coexist with such rules. The Commission's unsupported repetition of these talking points is wholly inadequate to satisfy its obligation on remand.

B. Real-World Experience Belies the Commission's Naive Belief that Unregulated Market Actors Will Voluntarily Maintain Net Neutrality Practices

The complete absence of evidence for the *Order on Remand*'s assertion that the *2018 Order*'s "light touch" framework would spur ISP investment or innovation—and the substantial evidence that it did not—is reason enough to vacate the *Order on Remand,* given the serious public safety issues it implicates. But there is also clear evidence that ISPs have taken advantage of the Commission's abandoning the field of BIAS regulation: after the *2018 Order*, ISPs have blocked or throttled Internet traffic on discriminatory terms. On January 10, 2021,[50] an ISP that provides BIAS in northern Idaho and parts of Washington State, responding to Twitter's and Facebook's bans of former President Trump, announced in an email to customers entitled "Blocking Sites for Censorship" that it would begin blocking all of its customers from Twitter, Facebook, "and any other website that may also be [c]ensoring whether it be through their algorithm they use for their site or any other means." It later offered individual customers the option to opt out of the companywide block and then, faced with potential liability under a state net neutrality law, converted to an opt-in approach.[51]

As several media outlets accurately reported, the ISP's behavior did not violate any Commission rule, because the *2018 Order* had repealed prohibitions on ISP blocking Internet traffic based on its source or content.[52] Only Washington State could challenge the ISP's policy as unlawful because it enacted a statewide net neutrality law prohibiting this sort of discrimination.[53] While news reports of the ISP's decision to block Facebook and Twitter have focused on the political ramifications, public safety also hangs in the balance, because, as

---

[50] This occurrence took place after the last opportunity to present such matters to the Commission. *See* FCC Rule § 1.429(b)(1).

[51] *E.g.*, *Citing 'censorship' concerns, Idaho internet provider blocks Facebook, Twitter*, WKRC Local 12 (Jan. 13, 2021), https://perma.cc/658W-TM7H; E. Czachor, Internet Provider to Restrict Access to Facebook, Twitter to Customers Who Request It, Newsweek (Jan. 11, 2021), https://perma.cc/PC3D-Q8DV.

[52] *Id.*

[53] *Id.*; *see* Wash. Rev. Code § 19.385.020.

described above, social media platforms are now a critical component of local governments' effective and efficient emergency response. Moreover, if an ISP is willing to block major edge providers like Facebook and Twitter for political reasons, it may well also decide to block communications from local governments themselves.

Because public safety agencies rely on social media platforms to communicate with the residents they are charged with protecting,[54] an ISP's content-based blocking of Facebook, Twitter, and other social media platforms is dangerous enough in normal times. But the public's disconnection from social media, and the Internet more broadly, is even more dangerous in the midst of the COVID-19 pandemic during which people are shopping for necessities, working, and staying socially connected over the Internet. This is perhaps why, just months after shepherding through the *2018 Order*'s rollback of Net Neutrality Rules, the former chairman asked ISPs to voluntarily defer disconnecting customers in arrears, given the centrality of Internet access in the COVID era. Yet within a month of his touted "Keep Americans Connected Pledge," signatory companies had already begun disconnecting residential and small business customers for failure to pay, even though the COVID-19 pandemic had not abated.[55] It has just gotten worse in the months since. A December 2020 report[56] revealed that "nearly 3,000 anonymized consumer complaints filed with the FCC between June and August . . . [reflected] that the pledge wasn't as broadly effective as the agency claimed."[57] Even if expanded BIAS access would theoretically benefit public safety, the Commission has no answer for the fact that ISPs have left large swaths of the community, amounting to tens of millions of residents, many of them poor or in rural areas, disconnected from the Internet. If there were any theoretical basis to contend (as the Commission did in the *2018 Order* and again in the *Order on Remand*) that, freed from the Net Neutrality Rules, ISPs would dramatically expand access and thereby advance

[54] *Supra* Part II.A.

[55] *See* Santa Clara & Los Angeles April 20, 2020 Comment at 10 & nn.16-18.

[56] This report was published after the last opportunity to present such matters to the Commission. *See* FCC Rule § 1.429(b)(1).

[57] K. Griffis, *ISPs Say They Kept Virus Pledge, But Customers Disagree*, Law360 (Dec. 7, 2020), https://perma.cc/K7ZA-5QRB.

public safety, it is foreclosed by the fact that three years into the Commission's real-world test of the *2018 Order*'s guesswork, tens and tens of millions of people are still disconnected—and therefore unprotected by the public safety services that rely upon Internet access.[58]

IV. CONCLUSION

The evidence in the record before the FCC makes abundantly clear that Net Neutrality Rules are essential to public safety in the 21st Century. Those rules ensure that local governments can speak to and hear from the residents they are charged with protecting, maintain situational awareness during emergencies, activate and deploy first responders based on real-time information in the field, collaborate effectively to plan for and respond to emergencies, and take advantage of innovative and effective private-sector edge systems. The *Title II Order*'s Net Neutrality Rules prevented ISPs from undermining this public safety system by requiring them to carry residents' Internet traffic unblocked, unthrottled, and unimpaired.

Like the *2018 Order* that it endorses, though, the *Order on Remand* minimizes and undermines public safety agencies' reliance on their residents' robust and unfettered access to the Internet, disregards the irreparable harms to life and property that impaired Internet access can cause, permits ISPs to stifle the systems and markets that support public safety operations, and leaves public safety agencies far less equipped to respond effectively to emergencies. The *Order on Remand* does all of this in order to achieve a baseless and destructive deregulatory agenda. Indeed, in the face of evidence directly to the contrary, the *Order on Remand* claims that when ISPs are left unsupervised, they will act to protect public safety even when they must forgo revenue opportunities or political preferences to do so.

By prioritizing unsupervised markets over effective public safety operations, the *Order on Remand* violates the Commission's fundamental duty as the expert agency to which "Congress has given . . . the responsibility to regulate a market such as the telecommunications

[58] *E.g.*, J. Busby et al., *FCC Reports Broadband Unavailable to 21.3 Million Americans, BroadbandNow Study Indicates 42 Million Do Not Have Access*, BroadbandNow (Feb. 3, 2020), https://perma.cc/PWZ4-L2MY; *see also Order on Remand* at 93 ("more than 77 million people living in the United States lack a home broadband connection") (Dissenting Statement of Comm'r Starks).

industry that it has repeatedly deemed important to protecting public safety."[59] Indeed, "[o]ne of the fundamental premises of a regulatory scheme such as that established by the Communications Act is that the free market cannot always be trusted to" advance the public good.[60] The Commission has abdicated its regulatory duty by assuming otherwise.[61]

For these reasons, the *Order on Remand* must be reconsidered. Upon reconsideration, the Commission should reverse or vacate the *Order on Remand*, vacate the *2018 Order*, revert to the Net Neutrality Rules laid out in the *Title II Order*, and then, if necessary, consider what modifications to the *Title II Order*, if any, would further advance public safety.

Respectfully submitted,

JAMES R. WILLIAMS
County Counsel

/s/ Raphael N. Rajendra

Raphael N. Rajendra
Deputy County Counsel

Meredith Johnson
Deputy County Counsel

Phillip R. Malone
Juelsgaard IP and Innovation Clinic
Mills Legal Clinic at Stanford Law School

Jef Pearlman
Intellectual Property &
Technology Law Clinic
USC Gould School of Law

2354475.DOCX

[59] *Mozilla*, 940 F.3d at 60 (quoting *Nuvio*, 473 F.3d at 307).

[60] *Telocator Network of Am. v. FCC*, 691 F.2d 525, 549 (D.C. Cir. 1982).

[61] Much has been written about the 2018 episode in which Verizon throttled County Fire's mobile broadband Internet being used by a unit that was coordinating emergency response among several firefighting agencies combatting the then-largest wildfire in California history, and then refused to stop throttling until County Fire upgraded to a more expensive data plan. *See Order on Remand* at ¶¶ 46-47. The central relevance of this episode is not to contend that Verizon's actions would have violated the *Title II Order*, but instead to underscore that the *2018 Order*'s claim—repeated without reexamination in the *Order on Remand*—that ISPs will act to protect the public when left unsupervised is entirely baseless.