

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554**

In the Matter of:	
Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications	PS Docket No. 15-80
New Part 4 of the Commission's Rules Concerning Disruptions to Communications	ET Docket No. 04-35
The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers	PS Docket No. 11-82

**COMMENTS OF THE CALIFORNIA PUBLIC UTILITIES COMMISSION**

AROCLES AGUILAR  
HELEN M. MICKIEWICZ  
HIEN VO WINTER

320 W. Fourth Street, Suite 500  
Los Angeles, CA 90013  
Telephone: (415) 703-3651  
Facsimile: (213) 576-7007  
Email: [hien.vo@cpuc.ca.gov](mailto:hien.vo@cpuc.ca.gov)

August 26, 2016

Attorneys for  
The California Public Utilities Commission

**TABLE OF CONTENTS**

**PAGE**

I. INTRODUCTION ..... 1

II. BROADBAND NETWORK OUTAGE REPORTING ..... 3

    A. A Real Need for Mandatory Broadband Network Outage Reporting..... 3

    B. BIAS and Dedicated Services ..... 7

    C. Outages Caused by Unintended Changes to Software or Firmware or Unintended  
        Modifications to a Database ..... 9

    D. Metrics for Performance Degradation ..... 10

    E. Ensuring Reliable Access to 9-1-1 by the Disabled..... 13

    F. Confidentiality of Broadband Outage Reports ..... 14

    G. Information Sharing Practices of Broadband and Interconnected VoIP Providers .... 15

    H. Reciprocal Sharing of Information on Broadband Network Outages between State  
        and Federal Partners ..... 16

III. CHANGES TO INTERCONNECTED VOIP REPORTING RULES ..... 16

IV. CONCLUSION ..... 17

## I. INTRODUCTION

The California Public Utilities Commission (“CPUC” or “California”) submits these comments concerning proposals in the Federal Communications Commission’s (“FCC” or “Commission”) May 26, 2016 *Report and Order, Further Notice of Proposed Rulemaking [FNPRM], and Order on Reconsideration* to extend part 4 of the FCC’s rules regarding outage reporting to broadband internet access service (“BIAS”) providers and to update the part 4 rules applicable to interconnected Voice over Internet Protocol (“VoIP”) service providers. Specifically, the FCC seeks comment on (1) a proposal to address broadband network disruptions based on network performance degradation, (2) proposed changes to the rules governing interconnected VoIP outage reporting, (3) reporting of call failures in the radio access network and local access network, and on geography-based reporting of wireless outages in rural areas; and (4) refining the covered critical communications at airports subject to part 4 reporting.<sup>1</sup> These comments focus on the first two issues, as well as the implications of the *Report and Order/FNPRM* on the CPUC’s pending 2009 Petition in which the CPUC had requested direct, password-protected access to NORS for obtaining California-specific outage reports.<sup>2</sup>

---

<sup>1</sup> See *FNPRM*, at 3-4.

<sup>2</sup> See *In re Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Petition of the California Public Utilities Commission and The People of the State of California for Rulemaking on States’ Access to the Network Outage Reporting System (NORS) Database and a Ruling Granting California Access to NORS (“CPUC Petition”), filed Nov. 12, 2009, found at <http://fjallfoss.fcc.gov/ecfs/document/view?id=7020348021> (last visited 8/26/16). Since 2009, all facilities-based certificated and registered telecommunications providers in California must concurrently report to the CPUC all NORS reports electronically submitted to the FCC. See CPUC Decision (D.) 09-07-019, 2009 Cal. PUC LEXIS 320. It was, however, the CPUC’s preference to obtain NORS data directly from the FCC, but that option was not explicitly available under the FCC’s part 4 rules.

The CPUC supports the FCC’s proposal to extend part 4 outage reporting to broadband providers, “given BIAS’ ubiquitous penetration throughout the American landscape and the multiple important emergency and non-emergency uses for which Americans consume BIAS.”<sup>3</sup> The CPUC also supports the FCC’s proposed changes to the interconnected VoIP reporting rules that would require interconnected VoIP providers to report outages in a similar manner as other communications providers. To inform the FCC, the CPUC provides information on certain technical questions related to broadband networks, gathered as part of the CPUC’s broadband mapping program. This includes information related to measurements of packet loss, latency (delay), and number of server “hops.”

The CPUC, however, strongly opposes any suggestions that the FCC preempt a state’s ability to independently collect data, regardless of whether the data relates to broadband, wireless, or other communications services.<sup>4</sup>

---

<sup>3</sup> *FNPRM*, ¶ 111.

<sup>4</sup> The FCC has specifically recognized that states may have a need to collect detailed data about broadband networks, and that this is not incompatible with federal collection of the same or similar data:

[M]andatory State broadband information collection efforts would not necessarily conflict with those actions or with any other Commission action or policy. In fact, Congress recognized in the BDIA that State broadband data gathering can be “complementary” to federal efforts. Given the specific federal recognition of a State role in broadband data collection, we anticipate that State efforts will not necessarily be incompatible with the federal efforts or inevitably stand as an obstacle to the implementation of valid federal policies.

*National Association of Regulatory Utility Commissioners Petition for Clarification or Declaratory Ruling that No FCC Order or Rule Limits State Authority to Collect Broadband Data*, 25 FCC Rcd. 5051, at ¶ 9 (2010). To preempt the states would also interfere with the concept of “cooperative federalism.” *Global NAPs Inc. v. Verizon New England*, 444 F.3d 59, 72 (1st Cir., 2006) (1996 Telecommunications Act “divided authority among the FCC and the state commissions in an unusual regime of ‘cooperative federalism,’ with the intended effect of leaving state commissions free, where warranted, to reflect the policy choices made by their states”).

The CPUC continues to believe that direct access to the FCC’s NORS database should only be conditioned on a state’s certification that it has adequate confidentiality protections in place to protect NORS data, which California does.<sup>5</sup> In 2009, the CPUC petitioned the FCC for direct and secure access to California-specific NORS data in an effort to streamline the CPUC’s collection of outage data and to eliminate redundant reporting for entities required to concurrently provide the CPUC with California-specific NORS reports.<sup>6</sup> Similar to the FCC, the CPUC collects and analyzes outage data as part of its “traditional role of protecting public health and safety through monitoring of communications network functionality”<sup>7</sup> and treats this data as confidential. Any updated or new part 4 rules the FCC adopts should not prohibit or preclude states from adopting their own rules related to these matters. For example, in response to specific rural outages in California, the CPUC had recently considered updates or amendments to its service quality rules that would have included lower reporting thresholds than those in the FCC’s part 4 rules.<sup>8</sup> This example underscores the need for states to investigate and respond to state-specific outage issues as states see fit.

## **II. BROADBAND NETWORK OUTAGE REPORTING**

### **A. A Real Need for Mandatory Broadband Network Outage Reporting**

The CPUC agrees with the *FNPRM*’s observation that there is a real need for

---

<sup>5</sup> See, e.g., Cal. Pub. Util. Code § 583; see also CPUC Petition (Nov. 12, 2009), *supra*, at 18-20.

<sup>6</sup> CPUC Petition, *supra*, at 5-7, *passim*.

<sup>7</sup> *Id.*, at 14.

<sup>8</sup> See CPUC Service Quality Rulemaking (R.11-12-001), documents found at <https://apps.cpuc.ca.gov/apex/f?p=401:5:0::NO:RP,5,RIR,57,RIR::> (last visited 8/26/16).

broadband network outage reporting,<sup>9</sup> in that “[b]roadband networks now provide an expanding portion of today’s emergency and non-emergency communications and have technological flexibility that allows service providers to offer both old and new services over a single architecture.”<sup>10</sup> Both broadband and PSTN are offered over the same infrastructure. The distinction at the service level in how the bits are arranged for voice services – whether VoIP or traditional telephone service – is not one that most consumers can make. And, consumers should not have to draw such a distinction, as their expectations are for safe and reliable service. Whether the infrastructure that provides that service is the evolving 9-1-1 network, the evolving PSTN, or the evolving broadband environment, the evolution of technology should not supplant the gathering of information. As the FCC has repeatedly said, the evolution of the network in no way diminishes the Commission’s duty to preserve “the core statutory values as codified by Congress: competition, consumer protection, universal service, and public safety.”<sup>11</sup>

The CPUC agrees that broadband “outages and service disruptions can occur at both the physical infrastructure and the service levels. Broadband networks are just as vulnerable to physical outages and service disruptions as the public-switched telephone network (PSTN), but are also susceptible to attacks at the application layer, which may not affect the underlying physical infrastructure.”<sup>12</sup> The *FNPRM* correctly observes that

---

<sup>9</sup> See e.g., *FNPRM*, ¶¶ 93, 102, 103, 106, 111, 124.

<sup>10</sup> *FNPRM*, ¶ 102.

<sup>11</sup> See e.g., *Technology Transitions et al.*, GN Docket No. 13-5 et al., Report and Order etc., 30 FCC Rcd 9372 (2015) at ¶ 1; see also 47 USC § 151(1).

<sup>12</sup> *Ibid.*

“broadband networks’ interrelated architectural makeup renders them more susceptible to large-scale service outages” and that “[t]his new paradigm of larger, more impactful outages suggests that there would be significant value in collecting data on outages and disruptions to commercial broadband service providers.”<sup>13</sup>

This potential vulnerability of IP networks, manifested in the consolidation of call control functions as a part of the data server/cloud architecture, increases the impact of small errors at the core, resulting in outages which can have far-reaching impacts. The FCC, of course, has many examples of this from its NORS information. One illustrative example is a United Airlines routing problem that “degraded network connectivity for various applications,” resulting in the airline halting flights for about an hour and half in July of 2015.<sup>14</sup> In the case of VoIP, voice is the application which would be affected by a similar problem because the network architecture similarly concentrates functions.

The FCC says that “broadband networks can support centralized services, but, if not engineered well, they can harm resiliency objectives.”<sup>15</sup> California refers the FCC to its report on the April 2014 Multistate 911 Outage, when engineering for resiliency did not ‘fix’ the problem at the Intrado facility until Intrado personnel engaged the backup server. The critical server in Colorado *was* engineered for resiliency, because there was a backup in Miami, and the FCC’s report on the Intrado outage highlighted the

---

<sup>13</sup> *Id.*, ¶ 103.

<sup>14</sup> Network World “United routes root of outage to router”, July 8, 2015, <http://www.networkworld.com/article/2945798/router/united-routes-root-of-outage-to-router.html> (last visited August 19, 2016).

<sup>15</sup> *FNPRM*, ¶ 103.

communication problems in understanding the extent of the system failure. An additional layer to this communication problem is that it appears no alarm was set to a sufficient level of attention on the system to highlight that calls were not being routed. That reflects *both* a software development problem *and* an operational procedure problem.<sup>16</sup>

In the CPUC's experience, voluntary reporting does not work with all carriers. Carriers have argued against reporting to the CPUC, and although several argue that informal reporting is successful, the CPUC is aware of no evidence that this informal reporting covers all relevant outages.<sup>17</sup> Rules are required so that all carriers are treated equally, that consistent data is collected, and that carriers understand how to report uniformly.

Further, the claim that competition provides safe and reliable service because customers might have choice of carriers is an issue completely separate from the importance of outage reporting for public safety purposes. Questions about the existence of effective competition can continue where relevant, while the public safety mandate of the CPUC for access to reliable service and the reporting of outages remain paramount.<sup>18</sup>

---

<sup>16</sup> *April 2014 Multistate 911 Outage: Cause and Impact, Report and Recommendations*, Public Safety Docket No. 14-72, PSHSB Case File Nos 14-CC-001-007, at 9 (“NORS reports showed that Intrado has redundant capability to reroute 911 traffic through its Miami ECMC. ... After the problem was identified, Intrado personnel performed a manual switch to reroute 911 calls to the Miami ECMC to restore 911 call processing.”), found at <https://www.fcc.gov/document/april-2014-multistate-911-outage-report> (last visited 8/26/16).

<sup>17</sup> *See e.g.*, CPUC Rulemaking, R.11-12-001, AT&T Opening Comments to Proposed Decision issued November 12, 2015, at 2; Frontier Communications Inc., Opening Comments to Alternate Proposed Decision of Cmr. Sandoval issued June 22, 2016, Rulemaking 11-12-001, at 6.

<sup>18</sup> *See e.g.*, Cal. Pub. Util. Code §§ 451, 2896; *see also* CPUC Decision, D.15-08-041, 2015 Cal. PUC LEXIS 516, issued August 27, 2015, *Slip Op.*, at 3 (“Competition in the telecommunications market does not obviate the need for such service quality standards and reporting.”); *see also* R.11-12-001 (Service Quality), Order Instituting Rulemaking (OIR), issued December 12, 2011.

For these reasons, as well as those articulated in the *FNPRM*,<sup>19</sup> broadband reporting should be mandatory rather than voluntary, to ensure that the FCC has the necessary information to assess and respond to outages affecting critical infrastructure.

## **B. BIAS and Dedicated Services**

In the *FNPRM*, the FCC would require BIAS providers, for the first time, to provide broadband-specific outage information for dedicated services to further its public safety goals.<sup>20</sup> The *FNPRM* seeks comment on the view that its requirements “apply equally and neutrally regardless of technology or provider type.”<sup>21</sup>

Ensuring safety is of paramount concern to the CPUC,<sup>22</sup> and promoting technology-neutral outage reporting rules is also a shared policy goal.<sup>23</sup> Thus, the CPUC agrees with the *FNPRM*'s proposal to require comprehensive outage reporting,

that, for BIAS and dedicated services, would encompass: (i) all customer market segments to include – mass market, small business, medium size business, specific access services, and enterprise-class (including PSAPs, governmental purchasers, carriers, critical infrastructure industries, large academic institutional users, etc.); (ii) all providers of such services on a technology-neutral basis; and (iii) all purchasers (end users) of those services without limitation.<sup>24</sup>

---

<sup>19</sup> See e.g., *FNPRM*, ¶¶ 93, 102, 103, 106, 111, 124.

<sup>20</sup> *FNPRM*, ¶¶ 109, 110.

<sup>21</sup> *Id.*, ¶¶ 109, 110.

<sup>22</sup> See e.g., R.11-12-001 (Service Quality), Order Instituting Rulemaking (OIR), issued December 12, 2011.

<sup>23</sup> See e.g., *ibid*; see also D.06-08-030 (URF II), 2006 Cal. PUC LEXIS 367, *Slip. Op.*, at 36-38; see also generally D.09-07-019 (adopting GO 133-C), 2009 Cal. PUC LEXIS 320, *Slip. Op.*; see also Cal. Pub. Util. Code § 871.7 (universal service).

<sup>24</sup> *FNPRM*, ¶ 110.

The importance of dedicated services, formerly known as “special access, now referred to as Business Data Services” (BDS), has changed since the FCC adopted its part 4 rules. One reason is the changing architecture of wireless networks, which has evolved into one with many more types and sizes of cell sites in use, some of which have processing requirements within the network core and so require very fast connections. This proliferation of cell sites connects users to emergency services and every other location with which they want to communicate—and those cell sites are connected to the wireless network core with BDS. The increasing numbers of wireless devices make these networks even more important in the daily lives of Californians. The CPUC supports the technology neutrality component of the part 4 rules for all carriers, and supports NORS reporting by BIAS and access providers.

Further, the adverse impact of the failure of networks supporting critical infrastructure (emergency services, airports, etc.) operations frequently do not show up in NORS currently because 1) the failure thresholds affecting the application (voice or control system) frequently are not reached and 2) the end users are not identified as “critical infrastructure” (whereas, for example, 911 facilities are).<sup>25</sup> Communications to and among the facilities of critical infrastructure industries should be identified so that the users can plan for resiliency and monitor risk.

It is critical for the FCC and other public agencies to have situational awareness of public safety communications, wherever they originate and regardless of the kind of network delivering them. Public use of a network to make a voice call and the ability to

---

<sup>25</sup> Compare, e.g., *FNPRM*, ¶¶ 100-101.

contact critical resources (as defined by the FCC and the user) should be monitored as part of both the safety and public use mandate of the FCC.

**C. Outages Caused by Unintended Changes to Software or Firmware or Unintended Modifications to a Database**

As with events involving critical network element failure, the *FNPRM* proposes “to modify the NORS interface to support information regarding outages and disruptions that are associated with unintended changes to software or firmware or unintended modifications to a database.”<sup>26</sup>

Within a broadband network, it is important to distinguish between outages that occur at the physical layer and at the application layer in a broadband network because the best practices to mitigate or prevent the two types of outages in the future would necessarily be different.<sup>27</sup> One purpose the NORS database serves is to collect consistent data, for informing best practices, performing trend analysis, providing insights to vulnerabilities, and determining critical issues across carriers. Application layer attacks such as TDOS and DDOS events disrupt users’ abilities to use the facility, and so from that perspective, an outage is an outage. But understanding how the outage came to be is the best way to determine how to prevent it in the future. Personnel with each carrier might know their own network very well, but they do not know what is happening in the next network. In contrast, the perspective from the FCC’s database across carriers is both

---

<sup>26</sup> *FNPRM*, ¶ 124; *see also id.*, p. 126.

<sup>27</sup> *FNPRM*, ¶ 102 (“Broadband networks are ... susceptible to attacks at the application layer, which may not affect the underlying physical infrastructure”). “Over the top” VoIP, where the provider of the voice over Internet Protocol service is different than the provider of the physical infrastructure, presents different reporting challenges than does a facilities-based VoIP provider. *Id.*, ¶ 160, and fn. 404.

unique and critical for this purpose.

The CPUC supports requiring carriers to provide more specific reasons for outages because this information would better position the FCC to respond to individual failures.<sup>28</sup> Open fields are useful in the reporting format where further explanation is required, but they should not be substituted for areas which require an answer used for sorting information and/or developing best practices. For instance, the drop-down fields for root cause force carriers to choose a reason, where with an open field a respondent might be tempted to write the incredibly unhelpful response of “N/A.”

Further, in describing software outages, it is important to differentiate between a software design error of base code, which might be made by a manufacturer or R&D group who writes the code that runs the equipment, and a software configuration error, which is more likely to be made by network operations or field staff who are operating the equipment. Identifying this distinction would allow for best practices and discussions regarding both software development practices, which have changed considerably over the years, and operational practices, which are more often focused on behavior and mining data for performance and relevance. While there is natural overlap in the areas of automation and configuration, and OSS tools, these are still useful distinctions relevant for the development of mitigations and best practices.

#### **D. Metrics for Performance Degradation**

The FCC seeks comment regarding the FCC’s proposal in the *FNPRM* for

---

<sup>28</sup> *FNPRM*, ¶ 124.

measuring performance degradation that includes throughput, packet loss, and latency.<sup>29</sup> Based on CPUC staff’s review of data from the CPUC’s semi-annual mobile field tests, packet loss and latency can vary greatly, depending on a host of factors, including provider, network technology, location, and backhaul distance. The CPUC does not have a specific data collection threshold recommendation at this time. However, the CPUC supports the collection of performance degradation data, such as packet loss and latency, because this type of information has been useful in the CPUC’s data collection efforts to determine the availability of broadband in California. The FCC similarly may find this type of data useful in formulating best practices to address communications outages.

The CPUC has relevant data from its statewide mobile wireless field testing regarding the perception of an increasing number of carriers between a host and server.<sup>30</sup> The CPUC measures several parameters semi-annually at the same 1,990 locations, and beginning in the spring of 2015,<sup>31</sup> the CPUC introduced traceroute tests to its program.<sup>32</sup> Since that time, our analysts have observed the number of “hops” from one IP address to the next has increased significantly.<sup>33</sup> The data shows that to get from the same test

---

<sup>29</sup> FNPRM, ¶¶ 137, 138, 144.

<sup>30</sup> FNPRM, ¶ 144 (“We seek comment on a scenario in which the destination host is in on another provider’s network.”)

<sup>31</sup> For more on the CPUC’s mobile field testing program, refer to Comments of the California Public Utilities Commission, submitted September 15, 2015, *In the matter of Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, GN Docket No. 15-191.

<sup>32</sup> Traceroute documents the route on an IP network between client and server and logs the IP address of servers along the way. The CPUC has not presented traceroute results in previous comments to the FCC.

<sup>33</sup> A hop is a change of IP address, which can be seen using traceroute.

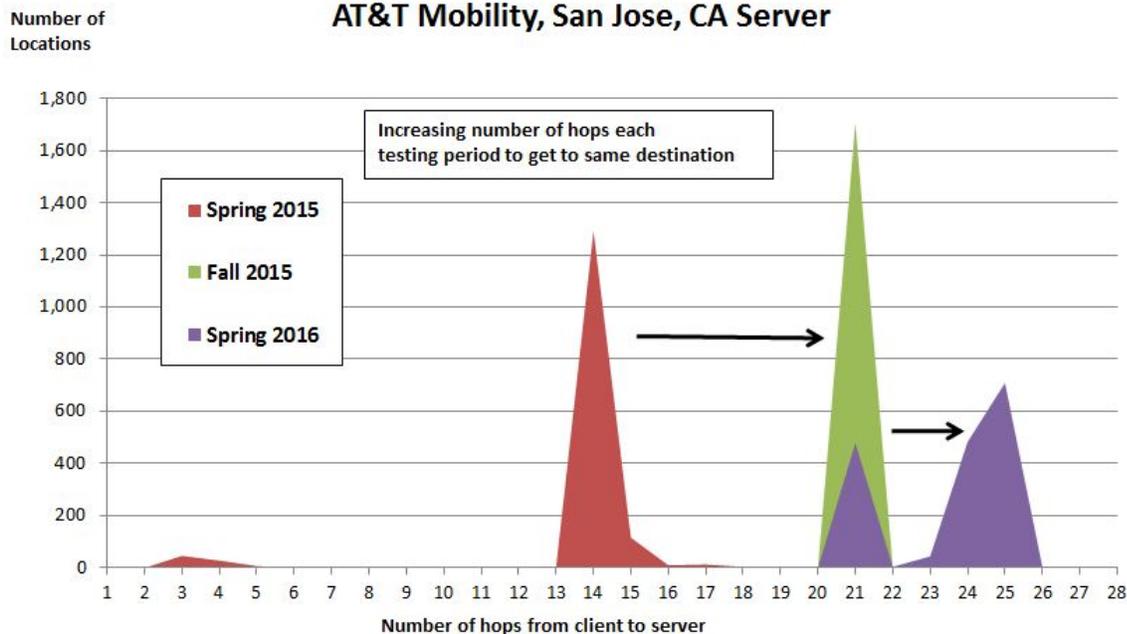
locations to the same content server in San Jose, California, the number of hops increased by over 70% over three rounds of testing.

There is not a clear correlation between the number of hops and the number of carriers, but the increase in the number of hops does point to an increasing number of servers between source and destination. The increased number of servers and the probability of one of them failing have the effect of increasing complexity in client-to-server communications, and potentially increases the likelihood of network element failure.

The following graph illustrates the increasing number of IP address hops, presumably each IP address representing a distinct server, to get from any of the 1,990 fixed testing locations via smartphone to the same server. The graph shows data for AT&T Mobility, and similar trends have measured for Sprint, T-Mobile, and Verizon Wireless.

The increase in IP addresses, and, presumably, servers, has occurred behind the scenes, invisible to the end user. As networks become more complex, troubleshooting problems in the event of a “hard down” outage is likely to become more complicated for BIAS providers.

## Number of Hops During TraceRoute Test AT&T Mobility, San Jose, CA Server



Based on traceroute test from each round of field testing (Spring 2015 through Spring 2016) for 1,990 locations across the state. Only locations with network connections are included. Samsung Galaxy S6 client.

### E. Ensuring Reliable Access to 9-1-1 by the Disabled

In the *FNPRM*, the FCC states,

[g]iven that video, text, and voice communications to 911 already traverse broadband networks and will continue to do so as the deployment of Real-Time Text and other NG911 multimedia applications grow, we believe that the CVAA’s [Communications and Video Accessibility Act of 2010] mandate for ensuring equal access to 911 provides an additional legal basis for the broadband reporting rules proposed herein.

The *FNPRM* seeks comment on this tentative conclusion and on whether “the proposed broadband reporting requirements are an ‘achievable and technically feasible’ way to meet this CVAA mandate.<sup>34</sup> The CPUC agrees.

<sup>34</sup> *FNPRM*, ¶ 200; *see also id.*, 199.

In comments on the FCC’s April 29, 2016 *Notice of Proposed Rulemaking on Transition from TTY [text telephone] to Real-Time Text Technology [RTT]*,<sup>35</sup> the CPUC noted the compatibility problems with the analog-based TTY legacy equipment being used over IP-based service – garbling, dropped calls, missed characters, and depending on the service provider, connection problems. Accordingly, the CPUC argued, it is important that RTT be interoperable with analog-based TTYs to ensure reliable access to 9-1-1 by the disabled.

#### **F. Confidentiality of Broadband Outage Reports**

The CPUC agrees with the *FNPRM*’s presumptive confidential treatment of broadband reports filed pursuant to part 4 rules.<sup>36</sup> Currently, the CPUC deems NORS outage reports that providers submit directly to the CPUC to be confidential and thus, it is reasonable to presume that broadband outage reports, which are to be submitted in NORS, should also be confidential.

While the CPUC remains committed to the FCC’s determination that information about outages in the telecommunications network should be kept confidential, California also notes that, because the public is directly affected, information about outages in the electric grid is not treated as confidential. The CPUC agrees with the *FNPRM* that the “approach of presumed confidentiality may need to evolve as networks, and consumer expectations about transparency, also evolve.”<sup>37</sup> This approach appropriately considers

---

<sup>35</sup> See CPUC Comments (August 5, 2016).

<sup>36</sup> *FNPRM*, ¶ 145.

<sup>37</sup> *FNPRM*, ¶ 145.

both provider and user perspectives. Here, because the public is directly affected by outages in the telecommunications network, it is appropriate for state commissions to have access to this information subject to confidentiality protections proposed in the CPUC Petition.

**G. Information Sharing Practices of Broadband and Interconnected VoIP Providers**

The *FNPRM* seeks comment “on the current reporting and information sharing practices of broadband and interconnected VoIP providers with state governments and other federal agencies.”<sup>38</sup> Since Cal. Pub. Util. Code § 710, which limits the CPUC’s authority over VoIP and IP-enabled services, became effective January 1, 2013, interconnected VoIP providers have cited to § 710 in generally objecting to provide the CPUC with any data regarding their interconnected VoIP services.

While § 710 does limit the CPUC’s regulatory authority, it also allows the CPUC to regulate where state or federal law expressly delegates authority to do so, or if the activity falls within one of the statute’s enumerated exceptions. Section 710(f) authorizes the CPUC to “continue to monitor and discuss VoIP services,” and recently the CPUC adopted a service quality rule requiring certain interconnected VoIP providers to provide the CPUC with copies of their NORS reports.<sup>39</sup> As discussed further below, the CPUC opposes any suggestion that the FCC preempt the CPUC’s state authority to

---

<sup>38</sup> *FNPRM*, ¶ 147.

<sup>39</sup> *See* fn. 8 (CPUC Service Quality Rulemaking, R.11-12-001).

independently collect data, regardless of whether the data relates to broadband, wireless, or any other communications service or technology.

#### **H. Reciprocal Sharing of Information on Broadband Network Outages between State and Federal Partners**

The CPUC supports the concept of reciprocal information sharing between state and federal agencies, as this is precisely what the CPUC sought in its 2009 Petition, which requests that the FCC share California-specific NORS data with the CPUC.<sup>40</sup> As explained above, the CPUC deems NORS data confidential and therefore would protect the data in a similar manner as the FCC. By petitioning the FCC for direct access to NORS, however, the CPUC in no way intended to waive its ability to seek this data independently and directly from providers pursuant to state law. Therefore, the CPUC strongly urges the FCC not to attempt to preempt states from the ability to obtain outage data directly from providers, as states see fit.<sup>41</sup> The CPUC has a state obligation to require that public utilities provide safe and reliable service and must be able to meet that obligation by collecting data that is specific to California's needs.

### **III. CHANGES TO INTERCONNECTED VOIP REPORTING RULES**

The CPUC agrees with the FCC's proposal in the *FNPRM* to have interconnected VoIP providers report in the same manner as legacy service providers.<sup>42</sup> Interconnected VoIP providers would file the same reports within the same time frames as other

---

<sup>40</sup> *FNPRM*, ¶ 148.

<sup>41</sup> See footnotes 4 and 5 and accompanying text, *supra*. Indeed, the CPUC would argue that the FCC lacks authority to prohibit the states, including California, from seeking any outage data independently under state law.

<sup>42</sup> See ¶¶ 127, 163.

applicable communications providers. This approach is consistent with the FCC's and CPUC's technology-neutral goals. These carriers are providing critical communications services, and customers frequently do not know the difference between VoIP and traditional telephone service or whether it is regulated or not. Indeed, even local governments, who may choose a VoIP service because it may be less expensive, may not realize the implications of this technology until an outage. Accordingly, safety rules, such as the part 4 outage reporting rules, should strive to be technology neutral.

#### **IV. CONCLUSION**

With this *FNPRM*, the FCC seeks to increase its “situational awareness” about outages that affect public safety and convenience and to promote technology-neutral reporting requirements. “Given the potential for broad-scale, highly-disruptive outages in the broadband environment – and particularly those impacting 911 service,”<sup>43</sup> the CPUC supports the FCC's proposed updates to its part 4 rules with respect to BIAS and interconnected VoIP service, as discussed herein. The CPUC agrees that “the adoption of updated broadband reporting requirements would likely provide the Commission with more consistent and reliable data on critical communications outages and enable it to perform its mission more effectively in light of evolving technologies and service offerings.”<sup>44</sup> The CPUC urges the FCC to continue to allow states to meet their similar, state-specific public safety and regulatory obligations by not preempting states' independent data collection efforts.

---

<sup>43</sup> *FNPRM*, ¶ 104.

<sup>44</sup> *Ibid.*

Respectfully submitted,

/s/ HIEN VO WINTER  
HIEN VO WINTER

Attorney for  
California Public Utilities Commission

320 W. Fourth Street, Ste. 500  
Los Angeles, CA 90013  
Telephone: (415) 703-3651  
Facsimile: (213) 576-7007  
Email: [hcv@cpuc.ca.gov](mailto:hcv@cpuc.ca.gov)

August 26, 2016