

**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

**REPLY 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: (213) 620-2021
Facsimile: (213) 576-7007
Email: hien.vo@cpuc.ca.gov

July 31, 2015

Attorneys for
The California Public Utilities Commission

TABLE OF CONTENTS

PAGE

I. INTRODUCTION 1

II. STATES’ ACCESS TO THE NORS DATABASE SHOULD BE MODELED
AFTER THE FCC’S SUCCESSFUL PROCESSES FOR SHARING
CONFIDENTIAL NUMBERING DATA AND CONFIDENTIAL
FORM 477 DATA WITH STATES..... 3

III. “LOSS OF COMMUNICATIONS TO PSAP(S)” PROPOSAL 9

IV. REPORTING OF WIRELESS OUTAGES 10

V. CONCLUSION 10

I. INTRODUCTION

The California Public Utilities Commission (“CPUC” or “California”) hereby replies to comments submitted in response to the Federal Communications Commission’s (“FCC” or “Commission”) March 30, 2015 *Notice of Proposed Rulemaking [NPRM], Second Report and Order and Order on Reconsideration* concerning proposed changes to the FCC’s network outage reporting rules.

The most significant proposal to California and other commenting state commissions, as well as the National Association of Regulatory Utility Commissioners (“NARUC”), is the FCC’s proposal to grant states “read-only access to those portions of the [Network Outage Reporting System] NORS database that pertain to communications outages in their respective states,” upon certification that the data will be kept confidential pursuant to confidentiality protections at least equivalent to those set forth in the Freedom of Information Act (“FOIA”).¹ None of the parties dispute the FCC’s position that “NORS data should be presumed confidential and shielded from public inspection.”² State and industry parties, however, disagree on how to protect NORS data from public disclosure.

Contrary to various industry comments,³ the FCC need not adopt any of the conditions, restrictions, requirements, or prerequisites discussed in paragraphs 52 and 53

¹ *NPRM*, ¶ 51, at 19.

² *NPRM*, ¶ 51, at 19.

³ See e.g., CTIA– **THE WIRELESS ASSOCIATION**® (July 16, 2015), at 13-15; Alliance for Telecommunications Industry Solutions (“ATIS”) (July 16, 2015), at 11-12; AT&T (July 16, 2015), at 25-30; Verizon (July 16, 2015), at 12-13; National Cable & Telecommunications Association (July 16,

of the *NPRM*, or any other additional recommendations, in order to adequately safeguard the NORS data. As the CPUC, the Massachusetts Department of Telecommunications and Cable (“MDTC”), the Michigan Public Service Commission (“MPSC”), the New York State Public Service Commission (“NYPSC”), and NARUC all note, the FCC already has adequate processes in place to protect confidential data maintained in other confidential FCC databases (i.e., Form 477 and North American Numbering Plan Administrator [“NANPA”]). The FCC has granted states direct access to those databases and California has successfully maintained the confidentiality of that data.⁴ The industry comments fail to demonstrate why these other secure processes, similar to that proposed in both the CPUC Petition and *NPRM*, would not sufficiently protect the NORS data.

With respect to the proposals related to Public Safety Answering Points (“PSAPs”), comments on the definition of PSAP degradation varied widely, which highlights the need for the FCC to clarify its rules. Significantly, The Association of Public-Safety Communications Officials-International, Inc. (“APCO”) supports the *NPRM*’s proposed clarification of “loss of communications to PSAPs”⁵ and the proposal to adopt “a separate and additional wireless outage reporting requirement based on the

2015), at 1-5; Comptel (July 16, 2015), at 8-10; Century Link (July 16, 2015), at 4-5; Competitive Carriers Associations (July 16, 2015), at 4-5; Sprint Corporation (July 16, 2015), at 11-14; XO Communications, LLC (July 16, 2015), at 7-8.

⁴ See *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”), ET Docket No. 04-35; RM-11588 (Nov. 12, 2009); see also CPUC Reply Comments (Mar. 19, 2010), ET Docket No. 04-35; RM-11588.

⁵ *NPRM*, ¶ 12, at 5.

geographic scope of an outage, irrespective of the number of users potentially affected.”⁶

The CPUC concurs with APCO. Whatever rules the FCC ultimately adopts, the CPUC urges the FCC to adopt rules that do not prohibit states from adopting their own rules as states deem necessary to perform their regulatory duties.

II. STATES’ ACCESS TO THE NORS DATABASE SHOULD BE MODELED AFTER THE FCC’S SUCCESSFUL PROCESSES FOR SHARING CONFIDENTIAL NUMBERING DATA AND CONFIDENTIAL FORM 477 DATA WITH STATES

The confidentiality concerns raised by industry comments in response to this *NPRM* were largely addressed in 2010 comments filed in response to the 2009 CPUC Petition, and further addressed by states’ and NARUC’s July 16, 2015 comments.

With its proposal to grant states access to the NORS database, the FCC addresses the CPUC’s 2009 Petition.⁷ The CPUC’s Petition sought “password-protected access to the NORS database...limited to California-specific disruption and outage data”⁸ and noted that the CPUC treats NORS reports it receives directly from reporting entities as confidential under state law and CPUC order.⁹ The CPUC tailored its request to be

⁶ *NPRM*, ¶ 34, at 13.

⁷ See *NPRM*, ¶ 49, at 18.

⁸ CPUC Petition, at 1.

⁹ CPUC Petition, at 18 (“The CPUC recognizes that public disclosure of disruption and outage data contained in the NORS reports poses serious implications to the nation’s critical information infrastructure. Therefore, consistent with the FCC’s treatment of NORS data, the CPUC ordered in D.09-07-019 that it would treat such information as confidential pursuant to the CPUC’s well-established protections under California Public Utilities (“P.U.”) Code § 583 and CPUC General Order (“G.O.”) 66-C.”).

consistent with the manner in which the FCC had been sharing confidential numbering and Form 477 data with California for years.¹⁰

In 2010, the FCC invited public comment on the CPUC Petition and received comments in support of the CPUC Petition from several state commissions, including Massachusetts, Missouri, and New York commissions, as well as the National Association of State Utility Consumer Advocates (“NASUCA”).¹¹ Many industry comments in 2010 did not object to granting states access to NORS; most, as here, claimed that additional confidentiality protections, beyond existing state confidentiality laws or orders, are necessary to adequately protect NORS data.¹² States’ comments in 2010, and States’ and NARUC’s comments in response to this *NPRM*, invalidate those claims.

For example, in 2010 the CPUC specifically responded to similar concerns raised by the Alliance for Telecommunications Industry Solutions (“ATIS”), the United States Telecom Association (“US Telecom”), AT&T, and the CTIA over California’s ability to safeguard NORS data. The CPUC stated,

In July 2009, when the CPUC conformed its requirements for reporting service outages and disruptions to the FCC’s, we required reporting entities to submit to the CPUC the same “highly confidential” data found in the NORS reports. We made explicit in Decision (D.) 09-07-019 (“Service Quality Decision”), that “[c]onsistent with the FCC’s treatment of

¹⁰ See CPUC Petition, at 15-20; see also CPUC Reply Comments (Mar. 19, 2010), at 5-6, 8-9.

¹¹ See *NPRM*, ¶ 50, at 18.

¹² See e.g., *generally* CTIA Comments (Mar. 4, 2010); ATIS Comments (Mar. 4, 2010); US Telecom Comments (Mar. 4, 2010); see also e.g., CTIA Comments (July 16, 2015), at 13-15; ATIS Comments (July 16, 2015), at 11-12; Verizon (July 16, 2015), at 12-13.

NORS data, we will afford the information confidential treatment pursuant to the Commission's well-established protections under Pub. Util. Code § 583 and GO [General Order] 66-C." Since then, the NORS data, as well as other confidential FCC data, remains protected, and will continue to be protected, under these laws. Furthermore, regulated carriers in California have been providing confidential and proprietary data to the CPUC under the protections of Section 583 and G.O. 66-C for decades. California's Public Records Act also has relevant confidentiality protection for critical infrastructure information.

ATIS, USTA, AT&T, and CTIA, all fail to substantiate their contention that California's existing confidentiality protections are inadequate to protect NORS data. Significantly, none of them identified a single instance in which the security of confidential data in the CPUC's possession was compromised in any way. In fact, the CPUC has been successful in safeguarding confidential data it receives from the FCC, including carrier-specific numbering resources data from the North American Numbering Plan Administrator (NANPA) and broadband data carriers provide to the FCC via Form 477.¹³

California Public Utilities Code section 583 makes it a criminal offense (misdemeanor) for any present or former officer or employee of the CPUC to divulge confidential information without a CPUC order.¹⁴ Since the CPUC has already by a CPUC order, deemed NORS data to be "confidential," consistent with the FCC's treatment of NORS data, it will be afforded the same level of protection in California as at the FCC.¹⁵

¹³ CPUC Reply Comments (Mar. 19, 2010), at 5-6 (citations omitted).

¹⁴ Pub. Util. Code § 583 ("No information furnished to the commission by a public utility, or any business which is a subsidiary or affiliate of a public utility, or a corporation which holds a controlling interest in a public utility, except those matters specifically required to be open to public inspection by this part, shall be open to public inspection or made public except on order of the commission, or by the commission or a commissioner in the course of a hearing or proceeding. Any present or former officer or employee of the commission who divulges any such information is guilty of a misdemeanor.")

¹⁵ See CPUC Reply Comments (Mar. 19, 2010), at 5-6.

State commissions' and NARUC's comments on the *NPRM* also point to the FCC's success in sharing confidential Form 477 and numbering data with states without the need for extra confidentiality protections.¹⁶ The MDTC notes, "as experience with the Form 477 and NANPA databases show, there is no need to place additional restrictions on a State's access to the NORS database, or limit a State's use beyond accessing only state-specific information....Adding supplemental requirements for access to NORS data or placing restrictive limitations on its use will discourage States from eliminating their own redundant reporting requirements. States could simply maintain duplicative direct reporting to safeguard their access to and analysis of outage information."¹⁷ To that end, states should have access to all NORS reports: notification, initial, final, and withdrawn reports.

The MCTC also cautions the FCC about preempting existing and future State outage reporting requirements: "State entities collect different information than is contained in the NORS database, and should not be foreclosed from making their own determinations as to whether data is duplicative...and it is unlikely that NORS data will adequately capture all the State's needs."¹⁸ California shares this concern; the CPUC is currently considering changes to the CPUC's outage reporting rules that may differ from the FCC's reporting requirements based on our state's specific service quality needs.

¹⁶ See MDTC (July 16, 2015), at 3; MPSC (July 16, 2015), at 4-5; NARUC (July 16, 2015), at 4-5.

¹⁷ MDTC (July 16, 2015), at 3-4.

¹⁸ *Id.*, at 5.

AT&T “questions whether state commissions truly require direct access to the NORS database to fulfill their missions.”¹⁹ On the other hand, many comments in 2010 and those submitted in response to this *NPRM*, acknowledge that outage and service disruption data is essential for state commissions to carry out their regulatory obligations.²⁰ In California, the CPUC has a statutory obligation to assess the reliability of the public communications network and to ensure that utilities provide a quality of

¹⁹ AT&T Comments (July 16, 2015), at 30.

²⁰ See e.g., NASUCA Comments (Mar. 4, 2010); City of New York Comments (Mar. 4, 2010); Massachusetts Department of Telecommunications and Cable Comments (Mar. 4, 2010); Public Service Commission of the District of Columbia Comments (Mar. 4, 2010); Missouri Public Service Commission Comments (Mar. 26, 2010); New York Public Service Commission Comments (Mar. 4, 2010); see also California Association of Competitive Telecommunications Companies (“CALTEL”) Comments (Mar. 8, 2010); ATIS Comments (Mar. 4, 2010), at 1 (“ATIS recognizes the legitimate needs of states to have access to outage reporting data”); The United States Telecom Association (“US Telecom”) (Mar. 4, 2010), at 1 (“US Telecom’s members recognize the legitimate interest that the California Public Utilities Commission (CPUC) has in obtaining federally-collected outage reports for its jurisdiction.”); see also e.g., ATIS Comments (July 16, 2015), at 11 (“ATIS NRSC does not oppose the sharing, with appropriate safeguards, of NORS data with states.”); Comptel Comments (July 16, 2015), at 8 (“There is no question that the public interest would be served if state governments were made and kept aware of communications outages within their borders so that they can take whatever action may be necessary to protect their citizens and promote the security, public safety and welfare of their residents.”); Century Link Comments (July 16, 2015), at 4 (“Century Link understands and appreciates state commission interest in NORS data”); XO Communications, LLC Comments (July 16, 2015), at 7 (“XO does not oppose the Commission granting states read-only access to portions of the NORS database that pertain to communications outages in their respective states so long as the same confidentiality requirements apply once the data is shared.”); NASNA Comments (July 16, 2015), at 2 (“NASNA supports the Commission’s proposal to grant states read-only access to those portions of the NORS database concerning outages in their respective states.”); NARUC Comments, at 4 (“As recent events confirm, communications network outages pose a significant risk to health and safety of the public. State agencies, including NARUC’s member commissions as well as State Offices of Emergency Services, are responsible for maintaining public services, including telecommunications services before, during, and after emergencies.”); Massachusetts Department of Telecommunications and Cable Comments (July 16, 2015), at 5 (“Direct access to the NORS database on a confidential basis will give State entities access to a significant additional resource, and will help advance State interests in protecting public health and safety.”); Michigan Public Service Commission Comments (July 16, 2015), at 7 (“Granting state agencies access to NORS outage information would permit states to perform their statutory duties in a more robust fashion, while enabling more efficient reporting practices for service providers.”); New York State Public Service Commission Comments (July 16, 2015), at 2 (“Direct access is warranted because understanding the entire scope, duration, and impact of an outage to a particular network or cluster of network elements is vital to situational awareness, especially in emergency situations.”).

service sufficient to support the safety, health, comfort, and convenience of the public.²¹

Outages affect, among other things, public access to emergency services, including 9-1-1.

As NARUC states, “all States share the need for immediate, secure and confidential access to the service outage detail provided in NORS. Comprehensive analysis of such data is key to understanding the impact of outages on multiple nodes of communication and data services which comprise each State’s communications networks.”²²

Accordingly, the *NPRM* correctly observes that “[g]ranting states access to NORS data on a confidential basis could advance compelling state interests in protecting public health and safety in an efficient manner.”²³

In sum, a state’s certification – that it will keep NORS data obtained from the FCC confidential and that it has confidentiality protections at least equivalent to FOIA – should be the only condition for a state to obtain direct access to the NORS database. The FCC should adopt the *NPRM* proposal in paragraph 51 without any of the additional requirements or restrictions discussed in paragraphs 52 and 53 or any of the other recommendations proposed by industry parties.

²¹ Public Utilities Code §§ 2889.8 and 451.

²² NARUC Comments (July 16, 2015), at 3 (emphasis in original).

²³ *NPRM*, ¶ 51, at 19.

III. “LOSS OF COMMUNICATIONS TO PSAP(S)” PROPOSAL

It is clear the FCC is asking the right question on the issue of how to determine what degradation or loss of communication to a PSAP looks like²⁴ because comments varied on the appropriate definition to be used. Both the NYPSC and the National Association of State 911 Administrators (“NASNA”) seek notification of any outage,²⁵ others request reporting when half the capacity is lost,²⁶ and some support the FCC’s proposal to notify when 80% of capacity is lost.²⁷ Some companies say that they are not able to determine when communications to a PSAP are lost,²⁸ and others propose to do nothing to clarify the rule.²⁹ Comcast Corporation proposed three possible definitions of what comprises degradation and limited those definitions to those which impact call processing for 9-1-1 calls,³⁰ but adopting these rules might not apply to all types of carriers delivering calls to PSAPs. The CPUC reiterates its support for a clarification of the rules, and one that is easy to implement, scalable to PSAP size, and capable of being reported consistently.

²⁴ See *NPRM*, ¶ 12, at 5.

²⁵ NASNA Comments (July 16, 2015), at 2; New York State Public Service Commission Comments (July 16, 2015), at 4.

²⁶ See e.g., APCO Comments (July 16, 2015), at 2.

²⁷ See e.g., XO Communications, LLC Comments (July 16, 2015), at 1.

²⁸ CTIA Comments (July 16, 2015), at 4; ATIS Comments (July 16, 2015), at 5; Sprint Corporation Comments (July 16, 2015), at 3.

²⁹ CenturyLink Comments (July 16, 2015), at 9; Verizon Comments (July 16, 2015), at 2.

³⁰ Comcast Corporation Comments (July 16, 2015), at 3.

IV. REPORTING OF WIRELESS OUTAGES

Both APCO and the CPUC support the FCC in adopting a requirement for reporting wireless outages based on geography.³¹ Sprint Corporation requested that the FCC refrain from adopting this rule.³² As APCO notes, this information would be helpful “during special events and tourist seasons that attract large crowds to areas that are otherwise sparsely populated.”³³ APCO further explains that this information would allow PSAPs to “plan for contingencies or mitigate potential harm to account for the lack of access to 911.”³⁴ As an organization representing public safety communications professionals, APCO has first-hand experience with issues that impact 9-1-1 and public safety communications networks.³⁵ The FCC should thus adopt the proposed additional wireless geographic-based reporting requirement in the *NPRM*.

V. CONCLUSION

The FCC should adopt its proposal to grant states access to NORS subject *only* to certification by a state that “it will keep the data confidential and that it has in place confidentiality protections as least equivalent to those set forth in the federal Freedom of Information Act (FOIA).”³⁶ Nearly all of the comments, including those from both industry and state representatives, agree that state commissions have a real need to

³¹ See *NPRM*, ¶ 34, at 13; see also APCO Comments (July 16, 2015), at 3; CPUC Comments (July 16, 2015), at 9.

³² Sprint Corporation Comments (July 16, 2015), at 8.

³³ APCO Comments (July 16, 2015), at 4.

³⁴ *Ibid.*

³⁵ APCO Comments (July 16, 2015), at 1.

³⁶ *NPRM*, ¶ 51, at 19.

receive NORS data and all concur that the data should be kept confidential. The additional “safeguards” discussed in paragraphs 52 and 53 of the *NPRM*, as well as those recommended in some industry comments, are overly burdensome and unnecessary. In California’s case, the CPUC has shown that industry concerns over California’s ability to safeguard NORS data, which the CPUC independently receives directly from its regulated entities, are unfounded.

California, the other commenting state commissions, and NARUC have also demonstrated that the FCC has successfully shared other confidential data through processes that require only a state certification of confidentiality similar to that proposed in the CPUC Petition and *NPRM*. The additional requirements or prerequisites recommended by industry parties are purported solutions in search of a problem and would unduly interfere with the ability of states to independently assess and respond to their state-specific needs.

On the proposed rules related to PSAPs, the CPUC supports the FCC’s clarification of what is meant by a “loss of communications to PSAPs.” The FCC should also adopt “a wireless outage reporting requirement based on the geographic scope of an outage, irrespective of the number of users potentially affected.”

///
///
///

By: /s/ HIEN VO WINTER
HIEN VO WINTER

320 W. Fourth Street, Ste. 500
Los Angeles, CA 90013
Telephone: (213) 620-2021
Facsimile: (213) 576-7007
Email: hcv@cpuc.ca.gov

July 31, 2015

Attorney for
The California Public Utilities Commission