

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of
New Part 4 of the Commission's Rules
Concerning Disruptions to Communications;
Petition of California Public Utilities
Commission and The People of the State of
California for Rulemaking On States' Access
to the Network Outage Reporting System
("NORS") and a Ruling Granting California
Access to NORS

ET Docket No. 04-35

RM - 11588

COMMENTS OF AT&T INC.

AT&T Inc., on its behalf and on the behalf of its common carrier subsidiaries, (AT&T) files these comments in response to the California Public Utilities Commission's (CPUC) petition for rulemaking and petition for access to the Network Outage Reporting System (NORS) database.¹

I. BACKGROUND

In 2004, the FCC² approved new network outage reporting rules that, among other things, extended mandatory outage-reporting requirements to all communications providers that provide voice and/or paging communications, provided a common matrix as a general outage-reporting threshold criteria, and simplified the criteria for reporting outages affecting 911/E911 and other special offices and facilities.³ At the same time, the FCC also modified the electronic filing systems used for submission of the outage reports.⁴ Now reporting entities can submit outage reports electronically through the FCC's web site, using a common outage reporting template. Data from these reports are maintained on the NORS database. That data includes both commercially sensitive and national security sensitive information, such as descriptions of the

¹ AT&T will refer the CPUC's two requests for rulings as the "Petition."

² To best distinguish between the Federal Communications Commission and the CPUC, AT&T will refer to the Federal Communications Commission as the "FCC" throughout this pleading.

³ *New Part 4 of the Commission's Rules Concerning Disruptions to Communications, Report and Order and Further Notice of Proposed Rulemaking*, 19 FCC Rcd 16830, 16834 (2004) (*Network Outage Reporting Order*).

⁴ *Id.*; see also, Public Notice, 19 FCC Rcd 24962 (Ofc. Eng. & Tech. Dec. 28, 2004).

causes of outages (including direct, root and contributing causes, as well as the effect of any lack of diversity), name and type of equipment that failed, the parts of the network involved, and location information. While reporting entities can access the NORS database to see their own previously submitted reports, reporting entities do not have access to the reports of others.

For its part, the CPUC concluded that it, too, needed data on outages affecting California service. The CPUC states in its Petition that AT&T and other carriers “supported California’s move towards reliance on the FCC’s NORS reporting scheme.”⁵ While AT&T worked with the CPUC to develop a reporting requirement regarding outages, AT&T did not support granting the CPUC direct access to the NORS database. In 2009, the CPUC approved an order that essentially adopted the FCC’s communication disruption and NORS reporting requirements and that required all facilities-based certificated and registered carriers to submit written reports to the CPUC for communication disruptions and outages that affect California service based on those requirements.⁶ Those written reports provide the CPUC with “all information electronically submitted to the FCC under NORS.”⁷

Now, the CPUC seeks direct access to the NORS database, asserting that the present arrangement is “unnecessarily duplicative and inefficient.”⁸ In support of its Petition, the CPUC contends that the present system, which requires CPUC staff to manually input “approximately 115 reports” a month into a database, is “neither a practical nor efficient use of staff resources.”⁹ It also alleges that “access to the NORS database would be relatively straight-forward” and that,

⁵ Petition, p. 6.

⁶ Decision Adopting General Order 133-C and Addressing Other Telecommunications Service Quality Reporting Requirements, California Public Utilities Commission Rulemaking Docket 02-12-004, Decision No. 09-07-019, 2009 PUC LEXIS 320 (2009) (*CPUC Outage Reporting Order*).

⁷ Petition, p. 7. To support the CPUC outage-reporting mandate, AT&T developed programming logic that gives the CPUC an efficient method of receiving, in real-time, FCC network outage report data associated with California service. Once AT&T inputs an FCC outage report—Notification, Initial, and Final—into the NORS database, the AT&T system packages the same outage data and forwards it by email to the CPUC point of contact.

⁸ Petition, p. 7

⁹ Petition, p. 12.

once it gained access to the database, that access would impose little, if any, burden on the FCC staff.¹⁰

For its part, AT&T believes that the FCC should carefully weigh the national security implications of the CPUC's proposals and make sure that all the necessary safeguards are considered. Efficiency and speed are all well and good but at the end of the day it is the duty of the FCC to guarantee the security of the "Nation's critical information infrastructure" and the special facilities that are served by it.

II. DISCUSSION

A. Protecting the telecommunications network is a critical function of the FCC's duties.

The FCC has acknowledged that the public needs "secure communications" for its day-to-day transactions, as well as during man-made and natural disasters.¹¹ Consequently, in the *Network Outage Reporting Docket*, the FCC held that the Communications Act itself authorizes the FCC to collect data for the purpose of guaranteeing the security of those communications needs. All parties involved in the *Network Outage Reporting Docket* immediately recognized that the outage reports would contain *commercially confidential information*. But more than that, the FCC and the commenters agreed that there were *critical security issues* in mandating network outage reports and maintaining a repository of data on those outages. The FCC noted that:

This data, though useful for the analysis of past and current outages in order to increase the reliability and security of telecommunications networks in the future, could be used by hostile parties to attack those networks, which are part of our Nation's critical information infrastructure.¹²

In a free and democratic society, it is part of our tradition to allow "open access to government information" and to foster "an informed citizenry." Yet, as noted by the comments

¹⁰ Petition, p. 13.

¹¹ *Network Outage Reporting Order*, 19 FCC Rcd at 16836-37 para. 11.

¹² *Id.*, at 16834 para. 3.

of the Department of Homeland Security (DHS), this tradition must sometimes give way to the primary role of government—protecting the public at large:

DHS understands that open access to government information and an informed citizenry are essential to the operation of our democratic system and to the missions of Federal agencies. However, as Congress has recognized, certain information that pertains to or affects our ability to protect the Homeland requires special safeguarding. Outage reporting data (particularly that requested by the FCC in the proposed template) constitutes such information.¹³

The information from outage reports that concerned the DHS included “information concerning the direct and root cause(s) and duration of the disruption; the range and types of services affected; the scope and gravity of the impact across all platforms and geographic area; specific equipment failures; the specific network element(s) impacted; remedial measures and/or best practices applied; and an appraisal of the effectiveness of the best practices.”¹⁴

In its Petition, the CPUC compares direct access to the NORS database with state-commission access to the semi-annual Numbering Resources Utilization Forecast (NRUF) reports and pass-word protected access to the North American Numbering Plan Administrator (NANPA) database.¹⁵ But the CPUC is comparing apples and oranges. It is true that there is an important and vital confidentiality interest in protecting NRUF data and the NANPA database. Carriers who are competing in the market place are required to surrender commercially sensitive data to the NANPA - the inappropriate disclosure of which could have serious *competitive ramification*. Nevertheless, the damage that could potentially result from the inadvertent or malicious disclosure of NRUF data and NANPA database information would pale in comparison to the damage that such disclosures of network outage report data could cause.

Depending on the disruption in question, the errant disclosure to an adversary of this [outage] information concerning even a single event may present a grave risk to the infrastructure. The potential availability of all reports, across all of the platforms proposed in the FCC’s Notice, could provide a potential adversary with a virtual road map targeting network stress points and vulnerabilities and a field guide to defeating “best practices” and protective

¹³ Comments of the Department of Homeland Security, p. 14 (June 2, 2004) (DHS Comments).

¹⁴ *Id.*

¹⁵ Petition, pp. 15-17.

measures. The FCC's apparent proposal to make the outage reports available to the public electronically over the Internet *increases this risk exponentially. Safeguarding this information—especially the location, root cause, provider and other sensitive information—should be a paramount consideration in the final rules adopted by the FCC.*¹⁶

While the CPUC's proposal does not include making outage reports available to the public over the Internet, it does increase the risks to the Nation's critical infrastructure exponentially by undoing the FCC's exclusive control over database access—vastly increasing the number of people who could access sensitive data. In lieu of the existing tight control over the NORS database that the FCC exercises today, the FCC would be allowing increasing numbers of people spread out over the entire country access to data the DHS argued requires special safeguarding.

Even with the NANPA database, the FCC imposed serious restrictions on state commission access. *First*, the FCC reiterated that the “confidentiality protections for forecast and utilization data adopted in the *First Report and Order* apply to state commissions when accessing carrier-specific data, whether in the form of semiannual reports or through the use of password-protected access.”¹⁷ *Second*, access was strictly limited to state specific data.¹⁸ Among other things, the FCC wanted to “ensur[e] that access will be granted only to state commission staff that uses this [numbering] data for area code relief purposes.”

For data that has national security implications, however, the FCC needs to think long and hard about the best ways to protect it from inadvertent and malicious disclosure or other inappropriate use.

¹⁶ DHS Comments, pp. 14-15 (emphasis supplied).

¹⁷ *Number Resource Optimization; etc., Third Report and Order and Second Order on Reconsideration in CC Docket No 96-98 and CC Docket No. 99-200*, 17 FCC Rcd 252, 310 para. 136 (2001) (“Specifically, state commissions must have appropriate protections in place (which may include confidentiality agreements or designation of information as proprietary under state law) that would preclude disclosure to any entity other than the NANPA or the Commission. Any state that cannot certify its ability to keep such data confidential shall not have access, password-protected or otherwise.”).

¹⁸ *Id.*, at 310 para. 137 (“[S]tate commissions’ access to reported utilization and forecast data should be limited to data concerning rate centers and NPAs within the requesting state, just as data in the form of semi-annual reports from the NANPA is so limited.”)

B. In light of the risks to critical infrastructure information, the FCC should impose stringent and rigorous conditions on any state commission access to the NORS database.

In the Petition, the CPUC recognizes that the inadvertent or malicious disclosure of NORS data could have dire results,¹⁹ but claims that it can adequately safeguard NORS data from public disclosure based on two purportedly “well-established protections” under California law: CAL. PUB. UTIL. CODE § 583 and CPUC General Order 66-C.²⁰

As for Section 583 of the CAL. PUB. UTIL. CODE, the CPUC points out that this section makes it a criminal offense (a misdemeanor) “for any employee of the CPUC to release confidential information to the public.”²¹ But as the Ninth Circuit has observed, Section 583 doesn’t bar the disclosure of anything:

As we read § 583, it is not a state statute that “forbids” disclosure of the [Appellant’s] reports within the meaning of § 1040(b) (1) [of the California Evidence Code]. *On its face, § 583 does not forbid the disclosure of any information furnished to the CPUC by utilities. Rather, the statute provides that such information will be open to the public if the commission so orders, and the commission’s authority to issue such orders is unrestricted. Moreover, even in the absence of an order by the commission, the information may be made public by an individual commissioner during a commission hearing.*²²

This section thus provides little or no protection to anyone producing critical data to the CPUC. This is so because the CPUC has free rein to make records and data publicly available and because CPUC commissioners may publicly release such data during public hearings, the protection allegedly afforded by Section 583 is not as strong as the CPUC asserts. Plus, in this case, a misdemeanor charge is not a sufficiently serious deterrent.²³

¹⁹ Petition, p. 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.”).

²⁰ *Id.* The CPUC asserts that in the *CPUC Outage Reporting Order* that it would treat outage reporting data as confidential.

²¹ *Id.*

²² In Re Subpoena Served on the California Pub. Util. Comm’n; et al. v. Westinghouse Electric Corp., 892 F.2d 778, 783 (9th Cir. 1989) (emphasis supplied).

²³ CAL. PENAL CODE § 19 (“Except in cases where a different punishment is prescribed by any law of this state, every offense declared to be a misdemeanor is punishable by imprisonment in the *county jail not exceeding six months*, or by fine not exceeding *one thousand dollars* (\$1,000), or by both.”) (Emphasis supplied).

General Order 66-C (GO 66-C), on the other hand, does appear to provide a little more protection—even though a critical part of it refers back to Section 583.²⁴ Among other records, GO 66-C excludes from public inspection “[r]ecords or information of a confidential nature furnished to, or obtained by the Commission” and “[n]on-public communications with other public agencies or officers where the public interest in withholding such records ‘clearly outweighs the public interest in disclosure.’”²⁵ Nevertheless, these CPUC provisions are subject to amendment by the state legislature and the CPUC and to interpretation by the CPUC and California state courts. Consequently, in spite of the CPUC’s assertions, the protections they provide can be largely illusory.

In Section 214, the Homeland Security Act protects critical infrastructure information *voluntarily shared* with the DHS and provided to the states by preempting state open-record laws.²⁶ To allow states access to NORS data without the same or equal protection would amount to an end run around the protections enacted by Congress to safeguard critical infrastructure. Plus, instead of a single federal standard governing the release and use of this data, the FCC would be in effect subjecting the data to the vagaries, political and legal, of multiple state jurisdictions. The FCC should enact a regulation similar to the DHS provision that would preempt state open-record laws governing the use and disclosure of any data obtained from the NORS database.

²⁴ CPUC General Order No. 66-C § 2.2 (June 5, 1974) (GO 66-C). This section cites to three different CAL. PUB. UTIL. CODE provisions: Section 583, discussed above, which appears to offer little real protection; Section 3709, which only applies to “highway carriers”; and Section 5228, which only applies to “household goods carriers.”

²⁵ GO 66-C §§ 2.2, 2.4.

²⁶ 6 U.S.C. § 133 (a) (1) (E) (“(a) Protection. (1) In general. Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)—... (E) *shall not, if provided to a State or local government or government agency—(i) be made available pursuant to any State or local law requiring disclosure of information or records; (ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or (iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.*”) (Emphasis supplied).

In addition to these “protections” under California law, the CPUC proposes the following additional safeguards:

- Password-protected access;
- Confidentiality status of carrier-specific data;
- Certification that appropriate protections are in place.²⁷

These proposals are neither specific nor sufficient. Given the nature of the risks involved measured against the CPUC’s claim that access to the NORS database is largely for its convenience, the FCC should take other and more efficacious steps to protect the nation’s critical infrastructure.

Limits on Number of Personnel. There should be a strict limit on the number of CPUC staff personnel who have access to the NORS database and information retrieved from it and the identities of state personnel with access should be on file with the FCC and kept current. First, as discussed below, this makes it easier to give persons with access appropriate training. Second, it makes it easier to discover the source of any inadvertent or malicious disclosure of critical information.

National Security Training. The CPUC should prepare and file with the FCC its training material for personnel with access to NORS database information. And the CPUC should provide the training before any access is granted. Among other things, the training ought to include information on why it is critical that data not be disclosed and what steps should be taken if personnel believe that data has been disclosed in violation of the privacy guidelines covering the acquisition of NORS database information.

Annual Certification. The CPUC should file an annual certification attesting to its adherence to the confidentiality guidelines, including its adherence to its training procedures and the requirement to keep current the list of personnel with NORS access. The certification should be attested to by an appropriate level state employee.

²⁷ Petition, pp. 16-17.

Restricted Use of Data. The CPUC’s use of data should be restricted to its stated reasons for requiring access; that is, it should be limited to evaluating the cause of outages in order to monitor communications network functionality:

NORS outage data contains information that would help evaluate the cause of the outages such as the April 9, 2009 incident in California. The CPUC could analyze the NORS data to determine whether an incident of this type is a one-time occurrence, outside the control of the utility. Alternatively, the incident might indicate a broader organic and/or systemic problem with certain facilities that should be investigated on a carrier-specific, industry-segment, or industry-wide basis to determine what, if any, corrective measures need to be taken. *California’s goal here is simply to obtain the data necessary to perform its traditional role of protecting public health and safety through monitoring of communications network functionality.*²⁸

This not only parallels the FCC’s rationale articulated in the *Network Outage Reporting Order*, but it also further safeguards the data by making sure that different organizations within a state commission are not getting access to the data. The data should be restricted to those who actually perform this evaluation function. What’s more, as the CPUC already has past information based on previously supplied reports, access to NORS data should be on a going-forward basis only.

In this same vein, state commissions should not have access to NORS data applicable to other jurisdictions. In the case of the CPUC, the duty to report network outages is restricted to “communication disruptions and outages that *affect California service.*”²⁹ Consequently, any state commission access to the NORS database and information should be limited to reports directly applicable to the state in question.³⁰

NORS Data Are Deemed Sufficient. The CPUC echoes the counsel of the FCC, which, when discussing making outage information available to the states, noted that state access would “reduce the reporting burden on communications providers.”³¹ This would only be so if the

²⁸ Petition, p. 14 (emphasis supplied).

²⁹ *CPUC Outage Reporting Order*.

³⁰ Compare access to NANPA database discussed at footnote 18 above.

³¹ *Id.* at p. 10, quoting from paragraph 25 of the *Network Outage Reporting Order*, which was citing DHS Comments at p. 8 (“DHS specifically recommends that the Commission explore methods to make outage information available to the State public utilities commissions (PUCs). Such information sharing would reduce the need for States regulators to collect intrastate outage data independently.”)

states adopt the FCC's reporting criteria and nothing more. Access to NORS then ought to be predicated upon the adoption of the FCC's Part 4 rules pertaining to network outages and the agreement not to impose more or different obligations on reporting entities. Naturally, this would mean that, before access is granted, existing state requirements would have to be withdrawn and supplanted by the FCC's reporting criteria.

III. CONCLUSION

Given the serious national security ramifications of the inadvertent or malicious disclosure of NORS data, the FCC should consider all reasonable steps to safeguard critical information infrastructure. Access to NORS data should only be granted when all parties—federal government, state governments, and reporting entities—are assured that the data is adequately protected.

Respectfully submitted,

/s/William A. Brown
William A. Brown
Christopher M. Heimann
Gary L. Phillips
Paul K. Mancini

AT&T Services, Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036
(202) 457-3007 (telephone)
(202) 457-3073 (fax)
William.Aubrey.Brown@att.com

March 4, 2010