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

REPLY COMMENTS OF AT&T INC.

Across the board, commenting parties agreed on one thing: if state commissions were to be given direct access to the NORS database, such access should be subject to some level of security precautions. Beyond that, there was a divergence of views. On the one hand, the service providers, who are obligated to submit confidential and security-sensitive outage reporting data, cautioned through their industry associations[1] that access should not be afforded lightly, emphasizing the significant risks to critical information infrastructure and the harm that can be unleashed by inadvertent or malicious disclosure of this data. These industry associations made multiple useful recommendations to the FCC for safeguarding this critical data. On the other hand, a few state commissions,[2] NASUCA,[3] and the City of New York, adopted the minimum measures proposed by the CPUC.

On balance—*i.e.*, in light of the potential harm to the nation and the relatively minor inconvenience to the state commissions—the recommendations of industry should be adopted if the FCC decides that access to the NORs database by state commissions is in the national

[1] The Alliance for Telecommunications Industry Solutions (ATIS), CTIA – The Wireless Association® (CTIA), and the United States Telecom Association (USTA).

[2] The Public Service Commission of the District of Columbia (DC-PSC), the Massachusetts Department of Telecommunications and Cable (MA-DTC), the Missouri Public Service Commission (MO-PSC), and the New York State Public Service Commission (NY-PSC).

[3] The National Association of State Consumer Utility Advocates.

interest. AT&T reiterates that the steps outlined in its Comments are the minimum steps needed to safeguard NORS data.

There were some comments, however, that would actively undermine the security of the NORS database, as well as repudiate the alleged bases for allowing direct access by state regulatory agencies to the NORS database in the first place. The FCC should not adopt those recommendations.

DISCUSSION

1. Use of NORS database information should be strictly limited to evaluating the cause of outages in order to monitor communications network functionality and not used to test marketing and advertising statements.

NASUCA proposes that state commissions be given direct access to the NORS database to "monitor the quality of service being provided to their citizens by communications providers."[4] It appears that NASUCA thinks that state commissions should test the "marketing and advertising statements" of the reporting entities to make sure they aren't misleading, overblown, or inaccurate.[5] This recommendation sounds consumer friendly and harmless. It isn't.

First, this recommendation would clearly undermine the FCC's aims of getting full and accurate data. Some carriers, concerned about how this data would be used, might be reluctant, or worse, to provide it. At the very least, such access would discourage frank and open disclosures by reporting entities to the FCC.[6]

Second, there is no one-to-one correlation between network outages and providing poor service. In the wireline world, where incumbent LECs, like the AT&T operating companies, are already held to high performance standards, reported outages are often not the result of any

[4] NASUCA Comments, p. 5.

[5] *Id.*

[6] AT&T doesn't mean to suggest that reporting entities would be concerned that advertising and marketing claims would be proven untrue. After all, their advertising claims are closely monitored by their competitors now. Any perceived deviations from the truth are quickly challenged in the appropriate arenas. Rather, AT&T is suggesting that reporting entities would be concerned that data from outage reports would give uninformed consumers an inaccurate and/or incomplete picture of the reliability of reporting entities' networks.

deficiency in the carrier's network or the result of the carrier's acts or omissions (*e.g.*, acts of nature, third-party acts).[7] In the wireless world, many reported outages don't involve any real interruption of service to actual end users (*e.g.*, DS3 simplex events that last more than five days after discovery—even when the DS3 has "switch[ed] to a protect-path within seconds of a failure of a primary path" and communications services are not adversely affected).[8] And, issues pertaining to coverage and speed—a mainstay of the wireless advertising wars—wouldn't be covered by outage reporting at all. It is naïve to think that NORS data provide an accurate picture of a service provider's overall quality of service or that a consuming public could draw reasonable conclusions from such data when evaluating competing advertising claims.

The FCC should reject any attempt to allow access to the NORS database and use of NORS data for any purpose other than the state commission's "traditional role of protecting public health and safety" through monitoring the network.[9]

2. Any proposed access to the NORS database should be limited to commissions entrusted with state-wide authority to regulate telecommunications providers within their jurisdictions.

The City of New York proposes that the FCC "grant all state public utility commissions *and local governments*, who can demonstrate the existence of adequate security measures, direct access to the network outage information contained in the NORS database in the same manner currently given to the DHS."[10] There is a serious question about whether the FCC should grant state commissions access to NORS and, if so, under what conditions. The suggestion that the FCC should grant local governments[11] such access is untenable.

---

[7] Acts of nature include storms, natural fires, fallen trees, rock slides, and floods. Third-party acts include cables cut during trenching activities, theft, motor vehicles hitting utility poles or pulling down overhead cables.

[8] *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Order Granting Partial Stay, 19 FCC Rcd 25039, paras. 1and 9 (2004).

[9] Petition, p. 14.

[10] The City of New York Comments, p. 3.

[11] The term "local governments" is not really defined. In addition to cities, like the City of New York, would that term include county governments? Would it include other state agencies or local commissions?

Cities are not generally charged with regulating telecommunications providers. State legislatures have entrusted that responsibility to state utility commissions. And the City of New York does not cite to any authority that gives it power over reporting entities.[12] In short, the City of New York doesn't have a role in monitoring the network.

AT&T can understand the City of New York's interest in being kept apprised of telecommunications issues affecting its citizenry and services, but the answer to this concern is not providing the City access to the NORS database. The City's concern can be addressed both by working with representatives of the state commission and developing emergency contacts with major carriers serving the community. Presumably one of the functions of the NY-PSC is to "ensur[e] safe and reliable telecommunications in New York."[13] To this end, the NY-PSC already has "existing outage reporting procedures."[14] The City can work with the NY-PSC to create lines of communications in order to allow the free-flow of accurate and appropriate information to the City in times of significant outages.[15] And nothing would prevent the City from contacting a carrier's liaison and obtaining information through that channel if appropriate.

There is significant danger of inadvertent or malicious disclosure of sensitive data pertaining to the nation's critical infrastructure information created by expanding the number of organizations with direct access to the NORS database. The risks of disclosure increase with each person entrusted with access. As cities do not have the obligation of regulating the reporting entities, there is no compelling reason to allow cities access to the NORS database and thereby increase the risks of disclosing sensitive data.

---

[12] Cable TV Providers often are franchised by local municipalities, but Cable TV Providers are only reporting entities for purposes of network outages to the degree that they provide circuit-switched telephony. As providers of circuit-switched telephony, Cable TV Providers would be telecommunications providers regulated by state commissions, not cities.

[13] NY-PSC Comments, p. 1.

[14] *Id.* at p. 2. Admittedly, the NY-PSC may not have jurisdiction over all reporting entities operating in the state, but if the FCC were to allow it access to the NORS database, there would be no need to allow the City of New York to have it, too, especially as the City itself has no jurisdiction over *any* of the reporting entities.

[15] In emergencies, it would be better to have the state commission acting as the focal point for information then to have that function spread around multiple jurisdictions.

3. If access to the NORS database is granted, it should only be on condition that the state commission has adopted the FCC's outage reporting requirements and agreed not to impose additional requirements on the reporting entities.

The MO-PSC forthrightly declares that, if given access to the NORS database, it "does not intend to replace [its] outage reporting requirements with the FCC NORS requirements."[16] Yet, this declaration flies in the face of the principal reason trumpeted by almost all commenters as a reason for allowing state-commission access to the NORS database: reducing the reporting burden on communications providers.[17] The MO-PSC asserts that

> State utility commissions should continue to have the authority to establish state-specific outage reporting requirements for carriers under the state commission's jurisdiction and as allowed by state law.[18]

By making this statement, MO-PSC removes any justification for granting the state commission access to the NORS database. It amounts to a case of all risk and no benefit.

MO-PSC recognizes this shortcoming in its position and contends that it needs access to NORS data because there are providers not covered by its existing outage reporting rules.[19] MO-PSC claims that it cannot fulfill its role in assisting the State Emergency Management Agency (SEMA) without this information. MO-PSC's recourse lies not in Washington, DC, but in Jefferson City, MO. The state legislature can simply pass a law that requires certain businesses within the state to provide contact information to SEMA for emergency situations. These contacts can keep SEMA apprised of the status of the affected networks in cases of emergencies. Duplicating outage reporting obligations across the nation is a bad trade off for NORS access. Accordingly, access to NORS 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.

---

[16] MO-PSC Comments, p. 2.

[17] *See*, Petition, p. 10; *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 para. 25 (2004) (*Network Outage Reporting Order*); Comments of the Department of Homeland Security, p. 8 in the *Network Outage Reporting Docket*. *See also*, ATIS Comments, p. 6; MA-DTC Comments, pp. 4-5; USTA Comments, pp. 5-6.

[18] MO-PSC Comments, p. 2.

[19] *Id.* Citing its Rule 4 (4 CSR 240-3.550(5)(D), MO-PSC explains that its outage reporting rules requires carriers to notify it of "any abnormal service conditions involving three hundred or more customers and lasting thirty minutes or more."

CONCLUSION

Were the FCC to grant the CPUC's Petition, it should adopt stringent security measures to protect against the inadvertent or malicious disclosure of critical infrastructure information and require reliance on the FCC's Part 4 rules—in place of additional or different state rules—as a precondition to access. The measures proposed by the CPUC and the other state-commission commenters, as well as NASUCA, and the City of New York, are insufficient safeguards.

Respectfully submitted,

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 19, 2010

CERTIFICATE OF SERVICE

I, Lacretia Hill, do hereby certify that on this 19th day of March 2010, a copy of the foregoing "AT&T Reply Comments" in ET Docket No. 04-35 and RM-11588 a was served via electronic mail or U.S. First Class Mail to the parties below.

/s/ Lacretia Hill

Deirdre Cheek
Thomas Goode
ATIS
1200 G Street NW
Suite 500
Washington, D.C. 20005

Michael F. Altschul
Christopher Guttman-McCabe
Rick Kemper
CTIA
1400 16th Street NW
Suite 600
Washington, D.C. 20036

Richard A. Beverly
Lara Howley Walt
Public Service Commission for the District of Columbia
1333 H Street NW
Suite 200 West Tower
Washington, D.C. 20005

Geoffery Why
Commissioner
The Massachusetts Department of Telecommunications and Cable
Two South Station 4th Floor
Boston, MA 02110

David C. Bergmann
Attorney for NASUCA
Office of the Ohio's Consumers' Counsel
10 West Broad Street, Suite 1800
Columbus Ohio 43215-3485

NAUSCA
8380 Colesville Road
Suite 101
Silver Spring, MD 20910

Peter Mc Gowan
General Counsel
Public Service Commission
State of New York
Three Empire State Plaza
Albany, NY 12223-1350

Mitchel Ahlbaum
Radhika Karmarkar
New York City Department of Information Technology
And Telecommunications
75 Park Place, 9th Floor
New York, NY 10007

Jonathan Banks
Robert Mayer
Kevin Rupy
USTA
607 14th Street NW
Suite 400
Washington, DC 20005