

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
New Part 4 of the Commission's Rules	)	WT Docket No. 04-35
Concerning Disruptions to Communications	)	
_____	)	RM-11588
	)	
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)	)	
and a Ruling Granting California Access to NORS	)	

**COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®**

CTIA – The Wireless Association® (“CTIA”)<sup>1</sup> hereby submits its comments in the above-captioned proceeding.<sup>2</sup> The Petition (“Petition”) submitted by the California Public Utilities Commission (“CPUC”) proposes that the FCC grant state regulatory commissions direct access to the Network Outage Reporting System (“NORS”) maintained by the Federal Communications Commission (“FCC” or “Commission”). CTIA urges the Commission to carefully consider the risks of unauthorized disclosure of NORS data accessed by state commissions to other parties. Should the FCC determine that it is appropriate to share outage data with requesting state regulatory commissions, it must implement effective, meaningful safeguards designed to protect that data and

---

<sup>1</sup> CTIA-The Wireless Association® ([www.ctia.org](http://www.ctia.org)) is an international organization representing the wireless communications industry. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products.

<sup>2</sup> 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) and a Ruling Granting California Access to NORS, RM-11588, Docket No. 04-35, DA 10-220 (Sept. February 2, 2010) (“Petition”).

mitigate the risks of unauthorized disclosures. These protections should include, at a minimum:

- Disclosing to carriers which parties access their confidential reports;
- Requiring notification to the FCC and then the service providers in the event of a data breach;
- Providing audit tools to identify data breaches and their sources; and
- Terminating access to parties that are unable to protect sensitive reports from disclosure.

The NORS system contains both notices and detailed reports of significant outages filed by carriers to the FCC.<sup>3</sup> The reports provide specific details including the direct and root outage causes, a description of the equipment involved, which telecommunications services were affected, how many customers were affected, how long it took to restore service, and how the restoration was effected.<sup>4</sup> In recognition that such detailed outage information could be used by terrorists or others seeking to intentionally disrupt communications, the FCC, the Department of Homeland Security (“DHS”), the CPUC, and communications carriers all agree that these reports must remain confidential.<sup>5</sup> The FCC therefore must carefully consider the risks of sharing the

---

<sup>3</sup> See generally 47 C.F.R. Part 4.

<sup>4</sup> See generally *New Part 4 of the Commission’s Rules Concerning Disruptions to Communications*, Report and Order, 19 FCC Rcd. 16,830 (2004). (New Part 4 Rules Report and Order)

<sup>5</sup> See, e.g., Petition at 18; 47 C.F.R. § 4.2; T-Mobile Reply Comments, ET Docket No. 04-35 at 4 (filed June 24, 2004); US Cellular Reply Comments, ET Docket No. 04-35 at 4-5 (June 24, 2004); Nextel Reply Comments, ET Docket No. 04-35, at 4-5 (June 24, 2004); Cingular Comments, ET Docket No. 04-35 at 10-13 (May 25, 2004); Sprint Comments, ET Docket No. 04-35 at 27-28 (May 25, 2004); CTIA Comments, ET Docket No. 04-35 at 9-11 (May 25, 2004); Letter of ExParte from Ann Berkowitz, Associate Director, Federal Regulatory Advocacy, Verizon to Marlene Dortch, Secretary, FCC ET Docket No. 04-35, at 5 (July 27, 2004); *Comments of the Department of Homeland*

data with state public utility commissions. The more parties that are granted access to a confidential database, the less “confidential” it inherently becomes. Sharing data with additional parties geometrically increases the risk of disclosure and makes it more difficult to identify the source of breaches.

**I. IF THE FCC DETERMINES IT IS APPROPRIATE TO SHARE DATA WITH STATE PUBLIC UTILITY COMMISSIONS, THE FCC MUST ESTABLISH AND REPORT ON SAFEGUARDS TO MAINTAIN CONFIDENTIALITY.**

As stated above, the FCC must carefully consider the ramifications of opening sensitive outage data to the CPUC or other parties seeking access. CTIA believes that if the data is to be shared, the Commission must evaluate the likelihood and costs of disclosure and whether any safeguards and countermeasures can be taken to mitigate these risks.

**A. Identify State Specific Risks Before Sharing Data.**

In its Petition, the CPUC cites the access it has had to Numbering Resources Utilization Forecast (“NRUF”) reports as evidence that it can adequately safeguard

---

*Security*, ET 04-35 at 13-15 (June 2, 2004); *Reply Comments of the Department of Homeland Security*, ET 04-35 at 2 (June 29, 2004)

“Foremost among its concerns, DHS continues to urge the Commission to make safeguarding the sensitive information that will be contained in the outage reports a highest priority. . . .Consonant with the homeland security principles that underlie this proceeding, the Commission should explore all available means to protect sensitive information from inappropriate disclosure to those who might use it to attack the telecommunications infrastructure. Consistent with the agencies’ mutual responsibilities under HSPD-7, DHS stands willing to work with the Commission to find a solution that appropriately safeguards the information while meeting the competing needs of all interested parties.” (internal citations omitted)

Id.

information gathered from NORS reports.<sup>6</sup> While the NRUF reports contain data on phone number blocks carriers have reserved and the utilization carriers have made of those resources, the value of this numbering data does not compare to the damage that could result if outage data is deliberately or inadvertently disclosed to the public. Unlike numbering data, as DHS has noted, NORS data could be used by terrorists to attack and shut down critical services.<sup>7</sup>

As the FCC requires before granting access to NRUF data, it also should require each entity requesting access to outage data to evaluate and report on the specific state laws and regulations that will be used to protect NORS data. Further, the Commission should analyze any Sunshine or public access laws that may put confidential reports collected through NORS at risk of disclosure.

**B. If NORS data Is to Be Shared, State Public Utility Commissions Must Notify the FCC and Service Providers When Providing Data to Third Parties Outside the Public Utility Commission's Direct Employ.**

In the Petition, the CPUC argues that NRUF data can be protected because "P.U. Code § 583 makes it a criminal offense for any employee of the CPUC to release confidential information to the public."<sup>8</sup> While CTIA believes that disclosure by a

---

<sup>6</sup> Petition at 2, 15-17, 19, 20.

<sup>7</sup> See *supra* note 5. See also Laura Blumenfeld, *Dissertation Could Be Security Threat; Student's Maps Illustrate Concerns About Public Information*, WASHINGTON POST, Tuesday, July 8, 2003, Page A1 (describing deep concerns of DHS, national security leaders, and telecom executives after briefing by Sean Gorman, whose university dissertation project generated detailed telecommunications infrastructure maps -- including the key points of vulnerability -- from publicly available government sources).

<sup>8</sup> Petition at 18.

CPUC employee to anyone would be a violation, instances may arise in which it is unclear whether divulging this information triggers an offense, *e.g.*, if the CPUC shared outage information with local police or an aid agency. Through a notification provision, the Commission and carriers can ensure this critical information is shared appropriately with only those parties that have a direct and urgent need to know.

**C. State Public Utility Commissions Must Agree to Limited Use of NORS Data.**

CTIA believes that if the data is to be shared, state public utility commissions must agree that they will only use NORS data consistent with the purposes for which it was provided by the carriers. In its Petition, the CPUC consistently states that this information will be used to “support California’s homeland security and emergency response functions,”<sup>9</sup> and that NORS data is necessary to “help evaluate the cause of outages ... 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. . . .”<sup>10</sup>

Any attempt by a state public utility commission to impose state-specific outage reporting requirements in addition to, or instead of, those associated with NORS is inconsistent with the underlying policy goal of a unified national standard for outage reporting.

---

<sup>9</sup> Petition at 2.

<sup>10</sup> Petition at 14.

**D. The Commission Should Implement Audit Processes for Access to NORS Data.**

The Commission should create and maintain an audit log for its NORS database, recording which data was accessed, when and by which parties. This audit log should be archived for several years to aid investigations after data breaches. In addition, an effective way to assure limited and appropriate access by state commission employees would be to verify that only valid and active accounts exist. Accordingly, the FCC should audit all of the accounts it has granted to state public utility commissions every six months. Any accounts that have not been used in six months should be shut down to reduce the security risk of maintaining large numbers of unused accounts. CTIA believes that if the data is to be shared, the Commission must make the results of the account audits available to the carriers that provide reports to NORS. Periodic reports should be provided that record how many active accounts are maintained by each public utility commission and the number of reports accessed by each. Upon request, and in a reasonable time frame, the Commission must furnish reports to carriers listing which state public utility commissions' accounts have accessed their NORS outage data.

**E. Public Utility Commissions Should Disclose Any Unauthorized Access of NORS Data to the Commission and All Affected Providers.**

CTIA believes that if the data is to be shared, and if there is a breach or suspected breach of data, the state public utility commission must immediately notify the Commission and all affected carriers of the breach. Without such notice, the Commission cannot assure the confidentiality of the data, nor can providers take appropriate action to protect facilities and services put at risk.

**F. The Commission Should Terminate NORS Access by Any Requesting Party in Whose Custody a Data Breach Has Occurred.**

As noted above, security and confidentiality of data is of paramount importance. With the privilege of access to NORS data comes the serious responsibility of adequately protecting that data. Accordingly, CTIA believes that if the data is to be shared, the FCC must rescind access to NORS data by a state public utility commission upon finding that a breach has occurred.

**G. The Commission Should Require an Executed Agreement With a Requesting Party Before Allowing Access to NORS Data.**

The FCC should memorialize conditions (B-F) through a formal and binding agreement between itself and any state public utility commission requesting NORS access. The measures highlighted above to protect data shared with state public utility commissions are crucial. As the Commission observed when it established NORS and made release of outage data presumptively exempt from disclosure under the Freedom of Information Act, the “release of this information could also make regulated entities less forthcoming in the information submitted to the Commission at a time when it is especially critical that we obtain full and accurate information in order to prevent harm to the communications infrastructure.”<sup>11</sup> Accordingly, if the Commission determines that sharing outage data is necessary, the Commission must establish concrete, enforceable safeguards to ensure that state public utility commissions accessing NORS protect the confidentiality of the data and use it appropriately.

---

<sup>11</sup> *New Part 4 Rules Report and Order*, 19 FCC Rcd. at ¶ 45

**II. THE COMMISSION MUST CAREFULLY CONSIDER THE TECHNICAL IMPLICATIONS OF GRANTING DIRECT ACCESS TO THE NORS DATABASE.**

In its Petition, the CPUC states that it only seeks reports on outages affecting California.<sup>12</sup> The NORS system requests that carriers list the geographic areas affected in the outage they are reporting. In the initial notification, the form requires a carrier to list a specific state or to simply list the outage as a “multi-state” event. In the initial and final report forms, carriers also must report a “More Complete Description of Geographical Coverage.” This system leaves quite a bit of ambiguity for reports from wireless carriers whose markets, switching areas, and systems often span state boundaries. If the Commission determines it is appropriate to share data with public utility commissions, the requesting commission must explain how it plans to parse reports and segregate data.

Specifically, the Commission should consider whether a public utility commission may be granted access to reports for outages originating from equipment that is not located in its state. When a multi-state outage does not affect enough customers within a particular state to meet the Commission’s outage reporting thresholds, the Commission should not grant access to the portion of the multi-state outage report that covers a state or states other than the requesting entity’s particular state. For example, it makes no sense to provide multi-state outage data to the CPUC if the incident at issue only created a 1,000 user-minute outage for customers in California.<sup>13</sup>

---

<sup>12</sup> See Petition at 1 (“[T]he CPUC requests password protected access to the NORS database; such access would be expressly limited to California-specific disruption and outage data.”).

<sup>13</sup> The current general case threshold for 900,000 user minutes. See 47 C.F.R. § 4.5.

Finally, there is the question of draft reports and withdrawn reports that reside in the NORS system. CTIA recommends that state public utility commissions only be given access to the completed reports. In their haste to file a timely response, carriers' draft reports often contain errors and discrepancies that need to be corrected. Moreover, carriers indicate that most withdrawn reports should not have been placed in the system or do not meet outage criteria. State public utility commissions should not have access to draft reports or withdrawn reports.

### **III. CONCLUSION.**

In formulating rules and procedures for sharing the highly sensitive and confidential records housed within NORS, the Commission must take significant precautions to safeguard the data. CTIA believes that if the data is to be shared, the system must include mechanisms that will allow the Commission to carefully monitor and audit NORS access, investigate data breaches, and terminate access to parties that fail to adequately protect the data they have accessed.

Respectfully submitted,

By: /s/ Rick Kemper

CTIA – The Wireless Association®  
1400 16<sup>th</sup> Street, NW, Suite 600  
Washington, D.C. 20036  
(202) 785-0081

Michael F. Altschul  
Senior Vice President and General Counsel

Christopher Guttman-McCabe  
Vice President, Regulatory Affairs

Brian M. Josef  
Director, Regulatory Affairs

*Its Attorneys*

Rick Kemper  
Director, Technology

Dated: March 4, 2010