

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

In the Matter of

Special Access for Price Cap Local Exchange Carriers;

AT&T Corporation Petition for Rulemaking To Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services

WC Docket No. 05-25

RM-10593

COMMENTS OF VERIZON AND VERIZON WIRELESS¹

The draft Protective Order² recognizes the need for special measures to protect from disclosure highly sensitive and confidential information that the Commission will request in the comprehensive data collection. Because some of this information is so sensitive from a competitive and network security standpoint, the Protective Order goes beyond previous protective orders in this proceeding and introduces new protections that limit how reviewing parties can access certain information. The Commission correctly concluded that these extra steps are necessary, and Verizon in these comments proposes only minor modifications to the Protective Order.

¹ In addition to Verizon Wireless, the Verizon companies participating in this filing are the regulated, wholly owned subsidiaries of Verizon Communications Inc. (collectively, “Verizon”).

² See Public Notice, *Wireline Competition Bureau Seeks Comment on Protective Order for Special Access Data Collection*, WC Docket No. 05-25, RM-10593, DA 13-1470 (June 28, 2013) (“*Public Notice*”) at Attachment, *Data Collection Protective Order* (“*Protective Order*”).

Specifically, the Commission:

- Should change its proposed designations to something less confusing than “Highly Confidential Data” and “Highly Confidential Information,” and
- Should not allow remote access to the Secure Data Enclave.

Designations: The *Public Notice* and the Protective Order distinguish between “Highly Confidential Information that is Highly Confidential Data” – which is subject to additional access restrictions and “Other Highly Confidential Information.”³ Creating an additional level of security for “Highly Confidential Data” is appropriate. Not only does some of the Highly Confidential Data constitute companies’ most competitively sensitive business information, it also includes information like network maps and locations served that if disclosed could compromise network security. But the designations “Highly Confidential Data” and “Highly Confidential Information” are ripe for confusion because they are so similar.

The Commission can easily avoid this potential confusion by changing the designations to make clear the distinction in levels of confidentiality and accordant protection. For example, the designations could be “Most Highly Confidential Information” and “Highly Confidential Information.” Regardless of the terms the Commission eventually adopts, the distinction between the two should turn on the level of confidentiality, not on the difference between “data” and “information.”

Secure Data Enclave: The Protective Order proposes that reviewing parties can inspect Highly Confidential Data in a secure data environment. This Secure Data Enclave should be a monitored physical clean room with no remote access, and computer systems in the Secure Data Enclave should not have connections to the Internet. That constitutes a more secure solution than a Secure Data Enclave with remote access through Virtual Private Networks. Ideally, computer

³ See *Public Notice* at 2, n. 9; see also Protective Order at Appendix A.

systems in the Secure Data Enclave would not have connections to computing or network systems outside of the physical room in which the Secure Data Enclave is located.

Limiting access to Highly Confidential Data to a monitored physical clean room significantly decreases the chances that someone could record Highly Confidential Data from screen views. While someone in a secure area conceptually could record data using a pen camera or a similar device, there is a risk of exposure in a monitored physical Secure Data Enclave. The chances of this occurring undetected are much greater at a remote location. A person located remotely using a VPN and a thin client has more opportunities to undertake optical data capture without detection or interference.

* * *

Respectfully submitted,

/s/ Curtis L. Groves

Michael E. Glover
Of Counsel

Christopher M. Miller
Curtis L. Groves
Verizon
1320 North Courthouse Road
9th Floor
Arlington, Virginia 22201
(703) 351-3084

July 29, 2013