

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Special Access Rates for Price Cap Local Exchange Carriers)	WC Docket No. 05-25
)	
)	
AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services)	RM-10593

**COMMENTS OF AT&T INC.
CONCERNING THE PROPOSED PROTECTIVE ORDER**

David L. Lawson
Sidley Austin LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

Robert C. Barber
Gary L. Phillips
Peggy Garber
AT&T Services, Inc.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-2121

Attorneys for AT&T Inc.

July 29, 2013

Table of Contents

INTRODUCTION.....1

DISCUSSION3

I. The Commission Should Continue To Use The Second Protective Order To Govern The Submission Of, And Access To, Highly Confidential Data In The Forthcoming Mandatory Data Collection Effort......3

II. The Proposed Protective Agreement Would Require Significant Modification Before It Could Be Adopted For Use In The Mandatory Data Collection Effort......7

CONCLUSION11

**Before the
Federal Communications Commission
Washington, D.C. 20554**

_____)	
In the Matter of)	
)	
Special Access Rates for Price Cap Local)	WC Docket No. 05-25
Exchange Carriers)	
)	
)	
AT&T Corporation Petition for Rulemaking to)	RM-10593
Reform Regulation of Incumbent Local)	
Exchange Carrier Rates for Interstate Special)	
Access Services)	
_____)	

**COMMENTS OF AT&T INC.
CONCERNING THE PROPOSED PROTECTIVE ORDER**

INTRODUCTION

This proceeding has to date been conducted under the auspices of two protective orders issued by the Wireline Competition Bureau. One, the *Second Protective Order*, was promulgated specifically to provide enhanced protection for “highly competitively sensitive” data, such as the locations of a provider’s last mile facilities and fiber network routes as well as existing and future business plans and strategies, that parties had been requested to submit in response to Commission’s previous voluntary data collection effort.¹ Recognizing the need to provide additional protections from public disclosure for such information, the *Second Protective Order* established processes by which a party could designate such data as “Highly

¹ *In the Matter of Special Access for Price Cap Local Exchange Carriers*, WC Docket No. 05-25, RM-10593, Second Protective Order (Dec. 27, 2010) (“*Second Protective Order*”), ¶2. Processes for designating, protecting and using “confidential” information in the proceeding are governed by a separate protective order that was originally issued by the Bureau in 2005 and subsequently modified in 2010. That latter order, the *Modified Protective Order*, also remains in effect. *In the Matter of Special Access for Price Cap Local Exchange Carriers*, WC Docket No. 05-25, RM-10593, Modified Protective Order (Oct. 28, 2010).

Confidential,” and generally limited the availability of information that has been so designated to a party’s outside counsel of record, the counsel’s employees, and the parties’ outside consultants, provided those counsel and consultants are not involved in “competitive decision-making activities.”² The Bureau concluded that the protections adopted in that order “will give appropriate access to the public while protecting a Submitting Party’s competitively sensitive information, and will thereby serve the public interest.”³

There has been no indication that conclusion was wrong. To the contrary, it appears that in the two and one-half years that the *Second Protective Order* has been in effect it has successfully advanced the Commission’s goal of protecting information that parties deem to warrant Highly Confidential treatment while still providing parties with reasonable access to that data for the purpose of litigating this proceeding. Nevertheless, and notwithstanding the continued viability of the *Second Protective Order*, the Wireline Competition Bureau now proposes to implement yet another protective order that ostensibly would govern the submission and review of information parties would submit in response to the pending mandatory data collection effort that the Commission initiated in its December 18, 2011 Report and Order and Further Notice of Proposed Rulemaking.⁴

As described below, this proposed new protective order has the potential to unnecessarily complicate – and possibly impair – the process of obtaining access to Highly Confidential information, especially data in electronic format. Accordingly, the Bureau should not proceed

² *Id.*, ¶¶3-6.

³ *Id.*, ¶3.

⁴ Wireline Competition Bureau Seeks Comment on Protective Order for Special Access Data Collection, *Special Access for Price Cap Local Exchange Carriers*, WC Docket No. 05-25, RM-10593, Public Notice (rel. June 28, 2013) (“*Notice*”). The proposed protective order, entitled “Data Collection Protective Order,” is set forth as an Attachment to the *Notice*.

with it, but rather should continue to use the *Second Protective Order* for the mandatory data collection effort. If the Bureau still deems it necessary to adopt new confidentiality procedures to cover that effort, however, it must first modify the draft order to ensure that it provides parties to this proceeding with meaningful and efficient access to all of the data.

DISCUSSION

I. The Commission Should Continue To Use The Second Protective Order To Govern The Submission Of, And Access To, Highly Confidential Data In The Forthcoming Mandatory Data Collection Effort.

Significantly, the *Notice* does not identify any deficiencies in the *Second Protective Order* that would preclude its use in the forthcoming mandatory data collection effort. To the contrary, the *Notice* states that the *Second Protective Order* will “continue to govern the submission, review and use of *all other* confidential information and documents submitted in this proceeding.”⁵ But the *Notice* does not indicate that there are any issues unique to the forthcoming mandatory data collection effort that could not be addressed through the *Second Protective Order*, much less ones that would require the adoption of completely new processes applicable solely to that effort.

More to the point, the enhanced protections for competitively sensitive information that were established in *Second Protective Order* would plainly be appropriate for conducting the mandatory data collection. The data that is considered to be “Highly Confidential” under the *Second Protective Order* is essentially the same as that identified in the proposed new order.⁶

⁵ *Notice*, at 3 and n.5 (emphasis added).

⁶ The only readily apparent difference in the types of data requested is that the proposed mandatory data requests would seek data concerning special access pricing and revenues, which of course were not part of the voluntary data collection effort. *Compare Notice*, Attachment, Appendix A with *Second Protective Order*, ¶6. But parties on both sides of the special access debate have previously submitted extensive pricing information in this proceeding pursuant to the terms of the *Second Protective Order*, and the fact that the mandatory data collection effort,

And as the Bureau previously concluded, that *Second Protective Order* meets the twin goals of providing enhanced protection for competitively sensitive information and of providing reasonable access to the parties to the proceeding to access and analyze that data. In particular, that *Order* places significant restrictions on access to data that is deemed to be Highly Confidential, limiting its availability to a party's outside counsel, that counsel's employees, and the party's outside consultants, provided that none are involved in providing advice to that party regarding business decisions that involve competition with the party that submitted that data.⁷ All of those personnel – including the outside counsel's employees – appropriately are required to execute an Acknowledgment of Confidentiality. Submitting parties also are entitled to object to disclosing data to particular persons, and until those objections are resolved that person may not obtain access to the Highly Confidential Information.⁸

Just as importantly, the *Second Protective Order* establishes reasonable methods through which the outside counsel and consultants can obtain access to, and make meaningful use of, the Highly Confidential data. Under the *Order* an outside counsel or consultant can request, at its cost, a complete set of any documents submitted by a party.⁹ Moreover, they can obtain a copy of all information in electronic format, which can be loaded on to a computer at their offices for

at least as currently envisioned, would include pricing and revenue information does not warrant the issuance of an entirely new protective order. Moreover, as AT&T has previously explained, the Commission should not be pursuing this data anyway because the data sought has no practical utility in this proceeding and the proposed requests violate the requirements of the Paperwork Reduction Act. *See* Paperwork Reduction Act Comments of AT&T Inc., April 15, 2013, at 13-24. But insofar as the mandatory data collection effort ultimately does encompass such information, it can easily be accommodated within the scope of the *Second Protective Order*.

⁷ *Second Protective Order*, ¶9.

⁸ *Id.*, ¶12.

⁹ *Id.*

purposes of analyzing that data.¹⁰ Once the analysis is complete the data must be removed from the computer, but the results can be stored to a mobile data storage medium that the counsel and consultants again retain at their own offices.¹¹

In contrast, the new protective order proposed in the *Notice* would establish a much more cumbersome process that could impair the ability of parties meaningfully to participate in this case, particularly given the Commission's current proposal to ground its determinations in complex regression analyses of the very data at issue.¹² For example, although the proposed order would again limit access to competitively sensitive information to a party's outside counsel and consultants, that access would be available only at a "Secure Data Enclave" – a secure environment established by, and presumably at, the Commission.¹³ To be sure, there may be value in making all of the data submitted in the mandatory data collection effort available to the parties at a central repository. However, the draft order does not simply contemplate that this Secure Data Enclave would be the site for accessing that data – rather, it suggests that the

¹⁰ *Id.*, ¶13.

¹¹ *See id.*, ¶13.a and b.

¹² As AT&T previously has explained, the Commission should not pursue these regression analyses, as they go far beyond what is necessary in this proceeding, would raise a host of methodological and econometric difficulties that may prove insurmountable, are unlikely in the end to produce an administrable test for pricing flexibility, and would almost certainly mire the industry and the Commission in protracted and costly proceedings for years to come. Comments of AT&T Inc., Jan. 11, 2013, at 19-32. If the Commission nonetheless attempts such an analysis, both the law and sound econometric practice require complete transparency in the process to ensure that any results are statistically robust and that the analysis can be independently tested. This requirement for transparency requirement must also inform the protective order governing the proceeding, and especially the processes the Commission implements for making the data and the Commission's own analysis available for review and testing by the parties.

¹³ *Notice*, Attachment, ¶6. The *Notice* suggests that access might be made available through a virtual private network, but even in that case the accompanying restrictions on the outside counsel and consultant's ability to retain copies of the underlying data presumably would remain. *See id.*

parties' outside counsel and consultants also would be required to conduct *all analyses of that data at that site*. Indeed, and unlike the process set forth in the *Second Protective Order*, the draft order would preclude counsel and consultants from obtaining copies of some of the most critical information that will be submitted to the Commission.¹⁴ Moreover, the reviewers would only be able to print out and remove from the Secure Data Enclave the aggregated results of their analyses of that electronic data¹⁵ – although even this accommodation appears to be in tension with the *Notice*'s statement that, whether the data is reviewed in a secure data environment or through a virtual private network, “we would not allow parties to store or print data or analyses on a local device.”¹⁶

Similarly, and as noted, the *Second Protective Order* permits the parties' counsel and consultants to store the results of their analysis to a mobile data storage medium. But the proposed order states that counsel or consultants using the secure data site only will be provided with “computer space to *temporarily* store the results of any analyses,”¹⁷ and by its terms it makes no provision for storing the results of the analysis on anything other than paper. This suggests a process in which counsel and consultants will be forced to continually and inefficiently recreate the analysis they previously completed.

These processes are unnecessarily convoluted and appear to be far from easily administrable. The logistics of scheduling sufficient time for all parties' counsel and consultants

¹⁴ *Notice*, Attachment, ¶6 and Appendix A. The proposed order would permit counsel and consultants to obtain copies of Highly Confidential documents, but not of “Highly Confidential Data,” a defined term in the proposed order that encompasses such information as locations of last mile facilities, fiber network routes, collocations, and cell sites and backhaul facilities – all data that is available for copying under the *Second Protective Order*.

¹⁵ *Notice*, Attachment, ¶6.

¹⁶ *Notice*, at 2.

¹⁷ *Notice*, Attachment, ¶6 (emphasis added).

to access the data at the secure site and conduct their analysis – and then likely repeating that process at least several times – while also maintaining the necessary privilege for that work-product presents a significant challenge that the *Notice* does not even broach, much less attempt to resolve. Most importantly, the constraints on accessing and analyzing the information, and the complete prohibition on obtaining copies of substantial amounts of the data, necessarily will increase each party's costs of participation, perhaps prohibitively, especially if counsel or consultants must repeatedly travel from out of town to the Secure Data Enclave to conduct their review and analysis of the data.

In short, there is no apparent necessity for supplanting the processes adopted in the *Second Protective Order*, which already have proven successful in protecting competitively sensitive information and providing reasonable access to that data for purposes of litigating this proceeding. There is even less need for replacing those proven procedures with untried new processes that will unnecessarily impair participation. Accordingly, the Bureau should withdraw the proposed new protective order and instead continue to rely on the *Second Protective Order* in all aspects of this proceeding, including the forthcoming mandatory data collection effort.

II. The Proposed Protective Agreement Would Require Significant Modification Before It Could Be Adopted For Use In The Mandatory Data Collection Effort.

As described above, there are substantial concerns about the effectiveness of the proposed protective order in meeting the goals of the Commission in this proceeding, and especially in facilitating reasonable access to, and meaningful analysis of, the data that will be submitted in the mandatory data collection effort. In contrast, the *Second Protective Order* has already shown that it can provide the enhanced protection necessary for competitively sensitive information while also providing the parties – and by extension the Commission – with the

ability to effectively use that information to address the central issues in this proceeding. Nevertheless, insofar as the Bureau determines to move forward with its new proposed order it must substantially modify that document to resolve a number of problems that are apparent in the draft.

First, the Bureau must clarify that outside counsel and consultants will be permitted to print and share among themselves any analysis they perform at the Secure Data Enclave. As noted previously, there is a tension between paragraph 6 of the proposed order (stating that “Reviewing parties may print out and remove aggregated results of their analyses”) and the categorical statement in the *Notice* itself that the Bureau “would not allow parties to store or print data or analyses on a local device.” The Bureau should resolve this ambiguity by confirming the ability of the parties’ counsel and consultants under Paragraph 6 of the proposed order to print out and remove the results of any analyses from the secure site, and to share that analysis with fellow counsel, employees and consultants who have executed the appropriate Acknowledgment of Confidentiality.

Second, and similarly, the Bureau must modify Paragraph 6 of the proposed order to permit the results of all analyses, as well as any computer programs or other methods of arriving at those analyses, to be stored on a mobile data storage medium, as is already provided in the *Second Protective Order*. The draft order currently does no more than provide temporary computer space in the Secure Data Enclave, and requires counsel and consultants using that facility to print out the results. In order to efficiently and effectively analyze the voluminous data that is expected to be submitted pursuant to the mandatory data collection effort, outside counsel and consultants must be able to store their work securely and permanently. This cannot

be accomplished through either the temporary computer access or paper files envisioned in the proposed order.

Third, the Bureau must clarify what constitutes “analyses” that may leave the Secure Data Enclave. Is it only listings of regression output? Does it include datasets of regression coefficients? Datasets of residuals? In other words, will a party’s counsel and consultants have to turn all of their analysis into a presentation or other summary of their work product inside the enclave, but only be permitted to remove output/summaries from the site? Or, as would be more appropriate, will they be able to remove the component pieces from the site for purposes of preparing comments, affidavits and presentations on their own systems?

Fourth, before the Commission can proceed with the restrictions on accessing the data that are contemplated in the draft order it must resolve how it will provide the parties’ counsel and consultants with access to software programs such as SAS[®] and Stata[®]. The *Notice* indicates that the Bureau is “exploring” how to provide access to their programs, but gives no indication when it expects to have resolved that issue. Access to both of those programs, as well as any other software packages that parties indicate they would like to use, will be key to the parties’ ability to properly analyze the data.

Fifth, the *Notice* suggests that the Bureau contemplates requiring “that data research results conform to one or more standard rules for identifying disclosure risk before permitting those results to leave the secure environment.”¹⁸ It should not impose any such requirement. Indeed, it is anything but clear how the Commission could enforce such a restriction, other than by reviewing that output before it is removed from the secure site. Such a process not only

¹⁸ *Notice* at 3.

would be unworkable, it would infringe on the privilege of the counsel and consultants working under their direction that attaches to that work product

Sixth, and similarly, the Bureau should abandon any notion of “adjust[ing] the raw data that is viewed in the secure data enclave by techniques such as the addition of random noise to the numbers or other masking techniques while still allowing the code to run on the unadjusted numbers.”¹⁹ Even if the Bureau could implement this proposal, the “benefits” of doing so in terms of additional confidentiality protections are at best dubious, and certainly are outweighed by the complications such techniques would add to an already burdensome process. Indeed, the use of these techniques could adversely affect any analysis, especially if the “noisy” data is all that the counsel and consultants are permitted to print out and remove from the secure facility.

Seventh, the Bureau will need to address how the confidentiality of each party’s analyses will be protected, if – as seems to be the case – there is just one Secure Data Enclave. In particular, the Bureau will need to develop procedures to protect the parties’ intermediate work product in the event they are required to share the same workspace.

Finally, the Bureau will need to resolve issues surrounding the ability of the counsel and consultants to bring other data, such as public information or parties’ own internal/confidential data, to the “enclave” to use in preparing their analysis. It is likely that the parties will need to utilize such data as part of their review. The Bureau thus must address how that information will be protected, and how that data transfer will operate.

¹⁹ *Id.*

CONCLUSION

For the foregoing reasons, the proposed protective order should be withdrawn, and the mandatory data collection effort should be governed by the terms of the *Second Protective Order*. If the proposed order is not withdrawn, it should be modified and clarified in the manner described above.

Respectfully submitted,

David L. Lawson
Sidley Austin LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

/s/ Robert C. Barber

Robert C. Barber
Gary L. Phillips
Peggy Garber
AT&T Services, Inc.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-2121

Attorneys for AT&T Inc.

July 29, 2013