

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

In the Matter of

Communications Assistance for Law
Enforcement Act and Broadband Access and
Services

ET Docket No.04-295

RM-10865

**REPLY COMMENTS
OF BELLSOUTH CORPORATION**

BELLSOUTH CORPORATION

Angela N. Brown
J. Lloyd Nault, II

Its Attorneys

Suite 4300
675 West Peachtree Street, N. E.
Atlanta, GA 30375-0001
(404) 335-0724
(404) 335-0737

December 21, 2004

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY1

II. THE INDUSTRY SHOULD CONTINUE TO TAKE THE LEAD IN DEVELOPING CALEA STANDARDS AS INTENDED BY CONGRESS4

III. THE SCOPE OF A PROVIDER’S CALEA OBLIGATIONS VARIES WITH THE TYPE OF SERVICE AT ISSUE6

IV. THE COMMISSION MUST ADOPT REASONABLE COMPLIANCE DEADLINES THAT TAKE INTO ACCOUNT THE TIME NECESSARY TO DEVELOP STANDARDS, DESIGN PRODUCTS, AND DEPLOY CALEA SOLUTIONS IN CARRIER NETWORKS10

V. THE COMMISSION’S PROPOSED FRAMEWORK FOR CONSIDERING SECTION 109(B) PETITIONS IS FAR TOO STRINGENT12

VI. CALEA ENFORCEMENT LIES EXCLUSIVELY WITH THE FEDERAL COURTS..15

VII. REQUIRING PROVIDERS TO BEAR THE SOLE RESPONSIBILITY FOR CALEA IMPLEMENTATION COSTS IS INCONSISTENT WITH CALEA19

VIII. THE COMMISSION SHOULD ALLOW BUT NOT REQUIRE PROVIDERS TO USE TRUSTED THIRD PARTIES TO SATISFY THEIR CALEA OBLIGATIONS....20

IX. CONCLUSION.....23

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

In the Matter of

Communications Assistance for Law
Enforcement Act and Broadband Access and
Services

ET Docket No.04-295

RM-10865

REPLY COMMENTS

BellSouth Corporation, by counsel and on behalf of itself and its wholly owned subsidiaries (collectively “BellSouth”), respectfully submits these reply comments in response to the *Notice of Proposed Rulemaking* (“*Notice*”) issued in the above-captioned proceeding.¹

I. INTRODUCTION AND SUMMARY

Despite the voluminous comments filed responding to the *Notice* and the divergent interests of the various parties, there is overwhelming consensus that the goal of this rulemaking should be to provide meaningful surveillance capability to law enforcement within the boundaries of the CALEA statute. To best accomplish this objective, the government should work collaboratively with the industry to develop tailored solutions that do not exceed the scope of CALEA, are cost-effective, and recognize the technical realities that exist today.

The record demonstrates that the industry is willing to do its part. As BellSouth and others explained in their opening comments, the industry has a long history of assisting law

¹ *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, *Notice of Proposed Rulemaking and Declaratory Ruling*, 19 FCC Rcd 15676 (2004) (“*Notice*”).

enforcement to conduct electronic surveillance, and that cooperation continues today. The objections to many of the proposals set forth in the *Notice* are not intended to thwart or hinder law enforcement's efforts. Rather, BellSouth and others are merely pointing out the legal deficiencies that make the Commission's proposals susceptible to lengthy court challenges that would only delay clarity and resolution for both law enforcement and the industry.

The record also makes clear that the only way to lawfully achieve a number of the objectives sought in the *Notice* is through a Congressional amendment. Although many of the Commission's proposals, as written, may be appealing to law enforcement, they exceed the scope of CALEA and therefore may not be adopted. To the extent the needs of law enforcement have changed and communications technology has evolved since CALEA was enacted, law enforcement and the industry should work with Congress to amend the current law. In the absence of such an amendment, however, the Commission is obligated to act within the confines of the current statute.

In addition, it is important to remember that the Commission's refusal to adopt the overly expansive proposals in the *Notice* will not deprive law enforcement of its continued ability to conduct lawfully authorized electronic surveillance. Federal and local agencies will still have available to them multiple means to perform surveillance activities. Long-standing statutes other than CALEA obligate all providers (including information service providers) to assist the government in performing electronic surveillance (*e.g.*, the Omnibus Crime Control and Safe Streets Act of 1968; the Electronic Communications Privacy Act;² the pen register and trap and

² Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) and Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (together codified as amended in 18 U.S.C. §§ 2510-2522 and in other sections of 18 U.S.C.).

trace statute³). CALEA does not replace or supersede these general wiretap laws, but, rather, supplements them. Indeed, law enforcement has used – and continues to use – these general wiretap statutes to conduct lawful intercepts on broadband services that are outside the scope of CALEA. Thus, the Commission’s decision not to adopt law enforcement’s proposals to expand the scope of CALEA to cover all broadband services and providers will not preclude law enforcement from effectively defending the Nation against crime and terrorism.

To ensure adherence to the letter and spirit of CALEA, the Commission should take the following actions:

1. Allow industry standards-setting bodies, in consultation with law enforcement, to complete efforts to establish appropriate surveillance standards for broadband services, including determining what requirements are necessary to meet the statutory definition of call-identifying information for broadband transport, Voice Over Internet Protocol (“VoIP”) services, and emerging services;
2. Clarify and define the scope of a provider’s CALEA obligations based upon the information within that entity’s control and which that entity uses in order to provide its CALEA-covered services to its customers;
3. Establish a reasonable process for reviewing petitions seeking relief under Section 109 that does not undermine the protections afforded by Congress;
4. Establish a reasonable and realistic deadline for complying with any new regulations adopted in this proceeding;
5. Recognize that CALEA enforcement lies exclusively with the federal courts and refuse to establish a separate enforcement mechanism;
6. Find that the government should be responsible for CALEA implementation costs as CALEA benefits the entire Nation; in the event the Commission declines to adopt this conclusion, it should grant providers flexibility to recover CALEA implementation costs; and
7. Allow for the voluntary use of trusted third parties as a means for providers to satisfy their CALEA obligations subject to certain safeguards.

³ 18 U.S.C. §§ 3121 *et seq.*

II. THE INDUSTRY SHOULD CONTINUE TO TAKE THE LEAD IN DEVELOPING CALEA STANDARDS AS INTENDED BY CONGRESS.

The importance of the standards process is echoed time and time again by commenting parties, including the Department of Justice (“DOJ”).⁴ The DOJ appropriately recognizes that this rulemaking proceeding is not the proper forum to determine CALEA technical standards.⁵ As the DOJ and others point out,⁶ if standards are absent or deficient, CALEA provides a mechanism whereby a party may petition the Commission to establish technical requirements or standards.⁷ To date, no such petition has been filed for the services at issue in this rulemaking. Accordingly, in the absence of such a petition, the Commission is not authorized to engage in the “sufficiently significant, technically complex, and legally controversial”⁸ task of establishing CALEA standards.

In addition to the lack of a statutory basis for Commission involvement, there is no policy justification for the Commission to interject itself into the standards-development process at this time given the critical and on-going efforts to establish new standards and refine existing ones for packet-mode communications. As a number of parties point out, industry associations and standards-setting bodies have done a significant amount of work over the past decade to provide law enforcement with CALEA-compliant intercept capabilities that take into account new

⁴ See, e.g., BellSouth Comments at 15-19; DOJ Comments at 39; Telecommunications Industry Association (“TIA”) Comments at 9-11; United States Telecom Association (“USTA”) Comments at 8; United States Internet Service Provider Association (“US ISPA”) Comments at 30; Verizon Comments at 15-16.

⁵ DOJ Comments at 39.

⁶ See, e.g., BellSouth Comments at 19; DOJ Comments at 39; US ISPA Comments at 32.

⁷ 47 U.S.C. § 1006(b).

⁸ DOJ Comments at 41.

technologies.⁹ This work continues today. For example, a standard for voice-over-packet services that would expand beyond basic calls and provide support for supplemental services (*e.g.*, call forwarding, call waiting, etc.) is currently being developed in an ATIS committee. The projected completion date for this work is November 2005. In addition, TIA is working on a third version of the J-Standard (J-STD-025-C) that would provide additional support for packet-data capabilities of wireless technologies. The projected completion date of this effort is March 2005. Rather than interfere with or slow down the progress of standards-setting groups, the Commission should allow the industry, working together with law enforcement, to continue to drive the standards process as intended by Congress.¹⁰

In light of the foregoing, there is no need to create a new committee, group, or special expert.¹¹ No additional benefits are gained from establishing a redundant body to examine CALEA technical issues. As the record demonstrates, work is being done today by existing industry standards groups, and there is no need to reinvent the wheel or duplicate these efforts. If the Commission desires to be kept apprised of the developments occurring within these standards-setting groups, it could send a representative to observe the standards meetings or obtain meeting minutes or status reports from the various standards bodies. This approach is consistent with CALEA in that it allows the industry to continue to play the central role in driving the CALEA standards-development process as intended by Congress.

⁹ *See, e.g.*, BellSouth Comments at 15-19; DOJ Comments at 39; TIA Comments at 9-11; USTA Comments at 8; US ISPA Comments at 30; Verizon Comments at 15-16.

¹⁰ *See* 47 U.S.C. § 1006(a)(1); H.R. Rep. at 19, 1994 U.S.C.C.A.N. at 3499.

¹¹ *See* SBC Comments at 16-17.

III. THE SCOPE OF A PROVIDER'S CALEA OBLIGATIONS VARIES WITH THE TYPE OF SERVICE AT ISSUE.

Although there are a number of issues on which the industry and law enforcement disagree, there is an important area of consensus – the fact that providers of broadband Internet access, providers of IP-enabled services, and providers of Internet content do not have equivalent access to the same type of “call” data and information. The DOJ correctly acknowledges this point when it states that, subjecting broadband Internet access providers to CALEA as “telecommunications carriers” “does not necessarily mean that they are responsible for extracting all of the call-identifying information available within the subject’s packet stream, particularly if it pertains, for example, to VoIP services that the carrier does not provide but that its subscribers may use.”¹² Notwithstanding the incorrect conclusion that broadband Internet access providers are telecommunications carriers for purposes of CALEA, the DOJ correctly recognizes that the ability to access the various types of data and information contained in a single communication vary from provider to provider depending upon the type of service offered.

The Commission must take these differences into account when determining the scope of a provider’s CALEA obligations. Indeed, the Commission should define a service provider’s obligations under CALEA based upon the information that is both within that entity’s control and is routinely utilized by the provider to offer its CALEA-covered services to its end users. This approach is endorsed by a number of commenters including BellSouth and the United States Internet Service Providers Association (“US ISPA”) and is fully consistent with CALEA’s

¹² DOJ Comments at 7-8.

legislative history.¹³ According to US ISPA, “the natural reading of the statute is that [call-identifying information] is ‘reasonably available’ to a carrier only if it is used by a carrier in the course of serving the carrier’s customers.”¹⁴ Indeed, as Congress has stated:

The question of which communications are in a carrier’s control will depend upon the design of the service or feature at issue, which this legislation does not purport to dictate. If, for example, a forwarded call reaches the system of the subscriber’s carrier, that carrier is responsible for isolating the communication for interception purposes. However, if an advanced intelligent network directs the communication to a different carrier, the subscriber’s carrier only has the responsibility . . . to ensure that law enforcement can identify the new service provider handling the communication.¹⁵

Congress clearly recognized that there would be instances in which one carrier would not have sole access to the information sought by law enforcement. Under those circumstances, that carrier’s only responsibility is to identify the provider that does have such information available to it. BellSouth follows this approach today. For example, if BellSouth provides transport to a non-affiliated Internet service provider and law enforcement serves BellSouth with a wiretap order for the customer of that Internet service provider, BellSouth cooperates with law enforcement to identify the appropriate entity that would be able to provide the information sought by law enforcement.

Although the DOJ appears to recognize that the ability to access various types of information contained in a single communication can vary from provider to provider depending

¹³ BellSouth Comments at 20; US ISPA Comments at 19.

¹⁴ US ISPA Comments at 19.

¹⁵ H.R. Rep. at 22, 1994 U.S.C.C.A.N. at 3502.

upon the type of service offered, its broad application of the term “switching” to routers¹⁶ perhaps reflects a fundamental misunderstanding of network facilities. Switches and routers involve different functionalities that may be performed by different entities in the provision of Internet access or VoIP to an end user.¹⁷ In addition, the information available to, and utilized by, a provider engaged in switching and routing functions will necessarily vary. The broad application of CALEA obligations in this context ignores the different nature of communications in the circuit-switched and Internet environments.

For example, BellSouth provides underlying broadband transport service (*e.g.*, DSL) on a wholesale basis to various application/Internet service providers. These providers, in turn, may offer VoIP services or access to the Internet via passwords to their respective end users. BellSouth utilizes switches, not routers, to provide the underlying transport services. The VoIP providers or Internet service providers that purchase BellSouth’s transport service use routers in their networks in order to serve their end user customers.

As BellSouth points out in its comments, the switches used in the provision of its broadband transport service are not capable of processing or interpreting higher layers of information. Similarly, as US ISPA explains, broadband transport providers “typically do not process packets at a layer higher than the IP layer, or operate hardware or software that provides the ability to ‘break open’ packets and examine content at higher network layers.”¹⁸ Because of

¹⁶ See DOJ Comments at 8-9.

¹⁷ See Newton’s Telecom Dictionary (15th ed. 1999) at 679 (defining a “router” as “an interface between two networks” that is a “much more capable” device than a switch, employing “both bridging and routing protocols”), and at 755 (defining a “switch” as “[a] mechanical, electrical, or electronic device which opens or closes circuits, completes or breaks an electrical path, or selects paths or circuits”).

¹⁸ US ISPA Comments, Appendix A at 7; *see also* Verizon Comments at 9.

these technical constraints, the information available to BellSouth from its switches is very limited, regardless of whether the wholesale customer is providing retail Internet access service or VoIP service.

For a broadband transport provider, the only method of providing call-identifying “like” information that is “reasonably achievable” is the delivery of the entire bit stream of the subject from which law enforcement can extract the desired addressing information. Any higher or disaggregated levels of information are not reasonably available to the broadband transport provider because, as explained above, its switches are not able to process or interpret higher layers of information. Moreover, the broadband transport provider does not utilize such data in the provision of its service to its customers. Indeed, the broadband transport provider is unaware of even the type of traffic (*e.g.*, voice, data, content, signaling) being transmitted over its facilities.

Accordingly, a rule requiring entities offering broadband transport to provide law enforcement anything more than a full packet stream would necessitate a complete redesign of carrier networks. Today, as a transport provider, BellSouth’s network is designed for efficiency purposes to carry as much traffic from as many different customers as possible. This efficiency is achieved by aggregating the traffic of multiple customers at points as close as possible to the individual customer. As Global Crossing describes, broadband transport providers’ networks are dominated by large data transmission “pipes” thereby limiting the ability of these providers to isolate the individual communications of customers from the larger data stream traversing the providers’ transmission facilities.¹⁹

¹⁹ Global Crossing Comments at 11.

In light of these network realities and technical limitations, it is both consistent with CALEA and reasonable for law enforcement to seek information from the provider that has “readily available” access to such information. BellSouth agrees with US ISPA that, “given the significant technical complexities of available solutions, it may be simpler and more cost effective for law enforcement to simply request . . . signaling information and . . . call content directly from the VoIP provider [or application/Internet provider] that processes such information, rather than from the broadband access provider.”²⁰

IV. THE COMMISSION MUST ADOPT REASONABLE COMPLIANCE DEADLINES THAT TAKE INTO ACCOUNT THE TIME NECESSARY TO DEVELOP STANDARDS, DESIGN PRODUCTS, AND DEPLOY CALEA SOLUTIONS IN CARRIER NETWORKS.

In its comments, BellSouth supported a minimum two-year transition period to afford affected providers an adequate opportunity to become CALEA-compliant for packet-mode communications.²¹ Most parties opposed the Commission’s proposed 90-day compliance window as unreasonably short,²² and BellSouth strongly objects to the DOJ’s proposed 12-month deadline.²³

Although the DOJ previously recommended a 15-month compliance deadline when it filed its initial Petition for Rulemaking,²⁴ it has since shortened this deadline by three months

²⁰ US ISPA Comments, Appendix A at 7; *see also* Verizon Comments at 12.

²¹ BellSouth Comments at 29-30.

²² *See, e.g.*, BellSouth Comments at 29-30; Nextel Comments at 11; SBC Comments at 23-24; T-Mobile Comments at 25; USTA Comments at 13.

²³ *See* DOJ Comments at 57-58.

²⁴ *See* Joint Petition for Expedited Rulemaking, WC Docket No. 04-295, RM-10865, at 48 (filed March 10, 2004).

without any apparent justification. As BellSouth previously explained, a two-year timeframe is unlikely to allow sufficient time to complete the development of standards and to design, test, and install equipment and software for the host of new services the Commission proposes to subject to CALEA.²⁵ US ISPA similarly states that a 15-month compliance deadline is inappropriate, because it “fail[s] to take into account realistic service, equipment and software design cycles, or associated standards processes.”²⁶ Given that a 15-month deadline by which to achieve full CALEA compliance is aggressive, the shorter 12-month compliance period advocated by law enforcement is neither reasonable nor realistic.

BellSouth believes that there is some merit to the Telecommunications Industry Association’s (“TIA”) proposal that the Commission establish a minimum 18-month period after the release of a final order to allow providers to achieve “substantial compliance” with any new Commission rules.²⁷ Under TIA’s recommendation, “substantial compliance” would be defined “as the achievement of sufficient wiretap capability so that criminals could not use the service without the content of their communications being subject to interception.”²⁸ During the 18-month timeframe, standards-setting bodies would continue their work to define standards for the delivery of call-identifying information for broadband services. BellSouth submits that a separate deadline should be established for compliance with requirements to deliver call-identifying information upon completion of the standards work. Such a deadline must take into account the time necessary to design, install, test, and deploy new equipment and facilities.

²⁵ BellSouth Comments at 30.

²⁶ US ISPA Comments at 34.

²⁷ See TIA Comments at 8.

²⁸ TIA Comments at 8.

V. THE COMMISSION'S PROPOSED FRAMEWORK FOR CONSIDERING SECTION 109(B) PETITIONS IS FAR TOO STRINGENT.

The DOJ supports the Commission's narrow interpretation of Section 109(b), which lacks the flexibility and carrier protections afforded by Congress and establishes a virtually unattainable burden of proof necessary for relief when CALEA compliance is not "reasonably achievable." According to the DOJ, Section 109(b) "was only intended to be available in limited circumstances (*e.g.*, to small or rural carriers with no history of electronic intercepts)."²⁹ This reading of Section 109(b) is not supported by the plain language of the statute and should be rejected.

There is nothing in the text of Section 109(b) or CALEA's legislative history to indicate that relief is available only to a certain class or size of carriers and only under limited circumstances. Rather Section 109(b) permits any telecommunications carrier to petition the Commission for a finding that compliance with the assistance capability requirements of CALEA is not "reasonably achievable."³⁰ Further, this statutory provision sets forth the 11 factors the Commission must consider in evaluating a carrier's petition.

Had Congress intended to limit Section 109(b) relief to small or rural carriers, it would have explicitly done so. There are a number of contexts in which Congress has carved out specific exemptions for certain classes of carriers. For example, local exchange carriers ("LECs") with fewer than two percent of the Nation's subscriber lines are authorized to petition state commissions for a suspension or modification of various obligations imposed on LECs

²⁹ DOJ Comments at 67.

³⁰ 47 U.S.C. § 1008(b).

(e.g., resale, number portability, interconnection, etc.).³¹ In addition, Congress has authorized the Commission to exempt certain carriers or classes of carriers from contributing to the universal service support mechanism if their contribution to universal service would be *de minimis*.³²

Clearly, Congress was aware that it could exempt or provide relief to a limited class or category of carriers. Had Congress desired to restrict the availability of Section 109(b) relief to rural carriers or those of a certain size, it could have adopted language accomplishing this result. However, Congress did not do so. Consequently, the DOJ's assertion that Section 109(b) relief is only available in limited circumstances has no basis in the CALEA statute.

BellSouth also objects to the DOJ's suggestion that any Commission finding that compliance with CALEA is not "reasonably achievable" under Section 109(b) be limited in duration.³³ Specifically, the DOJ proposes that any grant of a Section 109(b) petition be for a temporary period of time, not to exceed a year.³⁴ Once again, this interpretation of CALEA is wholly inconsistent with the plain language of the statute.

Section 109(b) does not vest the Commission with authority to establish compliance deadlines under Section 109(b). A carrier that has met the "not reasonably achievable" standard of Section 109(b) for covered services is exempt from complying with the assistance capability requirements of CALEA, unless the Attorney General is willing to pay the costs to make such compliance possible. This exemption is neither limited in duration nor contingent upon meeting

³¹ 47 U.S.C. § 251(f)(2).

³² 47 U.S.C. § 254(d).

³³ See DOJ Comments at 67.

³⁴ *Id.* at 68.

a Commission-imposed compliance deadline. Section 109(b) clearly refers to the cost to modify carrier facilities deployed on or after January 1, 1995, whereas extensions of time to comply are addressed in Section 107 of CALEA.

If law enforcement seeks to subject a carrier to a compliance deadline, it may turn to the federal courts for enforcement relief under Section 1007, as intended by Congress. However, even if a court exerts its enforcement authority, it is statutorily obligated to establish both a reasonable time and conditions for compliance.³⁵ Moreover, a court may not:

- (1) require a telecommunications carrier to satisfy the demands of law enforcement to any extent in excess of the capacity for which the Attorney General has agreed to reimburse the carrier;
- (2) require a telecommunications carrier to comply with the assistance capability requirements if there has been a finding that compliance with the assistance capability requirements is not reasonably achievable; or
- (3) require a telecommunications carrier to modify any equipment, facilities, or services deployed on or before January 1, 1995 unless the government has agreed to pay the costs to upgrade the equipment or the equipment, facilities, or services have been replaced, significantly upgraded, or undergone a major modification.³⁶

Reading CALEA to give the Commission authority to limit the relief granted under Section 109(b) to a maximum period of a year would essentially give the Commission more authority than that given to the federal courts in enforcing CALEA. Such an outcome is unsupported by the statute.

First, Section 1007(c)(2) specifically prohibits a court from requiring a telecommunications carrier to comply with the assistance capability requirements if there has been a finding that compliance is not “reasonably achievable.” Interpreting CALEA as giving

³⁵ 47 U.S.C. § 1007(b).

³⁶ 47 U.S.C. § 1007(c).

the Commission authority to find, on the one hand, that compliance is not reasonably achievable, but on the other hand, mandate a compliance deadline would completely eviscerate the stated purpose of Section 109(b).

Second, Congress did not require courts to limit compliance deadlines to a maximum period when issuing enforcement orders. Rather, a court must evaluate each situation on a case-by-case basis to determine a reasonable deadline and reasonable compliance conditions. Specifically, CALEA requires a court to consider a number of factors, including: (1) the good faith efforts to comply in a timely manner; (2) any effect on the carrier's or service provider's ability to do business; (3) the degree of culpability or delay in undertaking efforts to comply; and (4) any such other matters as justice may require.³⁷ Clearly, the statute contemplates flexibility that the DOJ's proposal completely ignores.

In sum, the Commission should reject the DOJ's proposed framework for reviewing Section 109(b) petitions. All carriers are entitled to seek relief under this statutory provision, and if such relief is granted, the Commission may not impose a compliance deadline.

VI. CALEA ENFORCEMENT LIES EXCLUSIVELY WITH THE FEDERAL COURTS.

The Commission cannot – and indeed should not – establish its own CALEA enforcement mechanism as advocated by DOJ, which erroneously asserts that Congress “created two parallel and complementary regimes” for CALEA compliance and enforcement.³⁸ This assertion is legally flawed, as an overwhelming majority of the commenters including BellSouth

³⁷ *Id.* § 1007(b).

³⁸ DOJ Comments at 72.

have pointed out.³⁹ As the Center for Democracy & Technology states, the “Commission has no authority to alter the carefully balanced court enforcement process created by Congress under CALEA or create a separate enforcement process.”⁴⁰ Similarly, CTIA notes that “Congress left no room for an alternative enforcement mechanism with the Commission, especially one that includes none of the careful protections and safeguards that Congress included in CALEA to ensure that it was implemented in a reasonable manner.”⁴¹ This sentiment was recently echoed in an Inspector General audit of the Department of Justice; the report stated: “CALEA does not give additional [enforcement] powers to the FCC.”⁴² Thus, any effort by the Commission to use its regulatory authority to assume a CALEA enforcement role oversteps the bounds of the CALEA statute.

According to DOJ, the Commission derives independent enforcement authority from Section 229. For example, the DOJ argues that Section 229(c) authorizes the Commission to investigate and take enforcement action against carriers to ensure CALEA compliance.⁴³ The DOJ’s reliance on Section 229(c) is misplaced. Section 229 of CALEA merely addresses the

³⁹ See, e.g., BellSouth Comments at 38-40; Coalition for Reasonable Rural Broadband CALEA Compliance Comments at 13-15; CTIA-The Wireless Association (“CTIA”) Comments at 9-12; Nextel Comments at 11-12; SBC Comments at 24-25; Telecom Consulting Associates (“TCA”) Comments at 6-7; TIA Comments at 4-7; US ISPA Comments at 41-44; USTA Comments at 11-12; Verizon Comments at 25.

⁴⁰ Joint Comments of Industry and Public Interest Comments (Center for Democracy & Technology) at 52.

⁴¹ CTIA Comments at 12.

⁴² Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, U.S. Department of Justice, Office of the Inspector General, Audit Division, Audit Report 04-19, at 23 (April 2004).

⁴³ DOJ Comments at 76.

Commission's authority to adopt rules regarding systems security and integrity procedures.

Specifically, Section 229(c) states as follows:

The Commission shall review the policies and procedures submitted under subsection (b)(3) of this section and shall order a common carrier to modify any such policy or procedure that the Commission determines does not comply with Commission regulations. The Commission shall conduct such investigations as may be necessary to insure compliance by common carriers with the requirements of the regulations prescribed under this section.⁴⁴

The Commission's investigative and "enforcement" duties under this provision are strictly confined to CALEA's system security and integrity requirements. There is no statutory basis for a more expansive reading of this provision.

CALEA clearly defines the Commission's authority, and general enforcement is not included among those powers. CALEA authorizes the Commission to:

- (1) designate certain types of entities as "telecommunications carriers" subject to CALEA;⁴⁵
- (2) exclude certain classes or categories of telecommunications carriers from the definition of a "telecommunications carrier;"⁴⁶
- (3) in response to a petition, establish technical requirements or standards for complying with the assistance capability requirements of CALEA;⁴⁷
- (4) grant extension requests;⁴⁸

⁴⁴ 47 U.S.C. § 229(c). Subsection (b)(3) of Section 229 requires carriers to submit to the Commission their policies and procedures designed to ensure that only authorized interceptions of communications and access to call-identifying information occur on the carriers' premises and that secure and accurate records of such activities are maintained. 47 U.S.C. § 229(b)(3).

⁴⁵ *Id.* § 1001(8)(B)(ii).

⁴⁶ *Id.* § 1001(8)(C)(ii).

⁴⁷ *Id.* § 1006(b).

⁴⁸ *Id.* § 1006(c).

- (5) establish rules regarding systems security and integrity;⁴⁹
- (6) in response to a petition, allow carriers to adjust charges, practices, classifications, and regulations to recover costs incurred to modify equipment for CALEA compliance;⁵⁰ and
- (7) in response to a petition, determine whether CALEA compliance is reasonably achievable.⁵¹

Any actions taken by the Commission beyond those articulated above are outside of the scope of the Commission's authority.

In addition to the legal infirmities described above, adoption of a separate enforcement mechanism with different compliance requirements and penalties imposed by the Commission would be duplicative and unduly burdensome on both carriers and the Commission. Congress specifically sought to avoid this outcome when it placed enforcement authority exclusively with the federal courts. According to CALEA's legislative history, Congress vested the federal courts with sole enforcement authority "[i]n order to avoid disparate enforcement actions throughout the country which could be burdensome for telecommunications carriers."⁵²

CALEA compliance is already challenging and costly without the added burden of disparate burdens of proof and duplicative enforcement mechanisms. Moreover, neither the Commission nor law enforcement has demonstrated a need for separate enforcement tracks. There is no evidence that the enforcement framework set forth in CALEA has failed or that the federal courts have not done their job. In fact, despite law enforcement's vociferous complaints about carrier non-compliance, BellSouth is unaware of any attempt by the government to seek

⁴⁹ *Id.* § 229.

⁵⁰ *Id.* § 229(e).

⁵¹ *Id.* § 1008(b)(1).

⁵² H.R Rep. at 28, 1994 U.S.C.C.A.N. 3489, 3508.

enforcement relief pursuant to the statute. Given the absence of authority, the existence of a statutory enforcement mechanism, and the potential for unduly burdensome and disparate requirements, the Commission should not seek to establish its own enforcement framework.

VII. REQUIRING PROVIDERS TO BEAR THE SOLE RESPONSIBILITY FOR CALEA IMPLEMENTATION COSTS IS INCONSISTENT WITH CALEA.

Commenters including BellSouth and TIA assert that electronic surveillance under CALEA is a public good that benefits the Nation and, as such, should be funded by the government or the general public.⁵³ Given the national interest in Homeland Security and the role played by CALEA in furthering this objective, it is more than reasonable for the government to bear the costs of CALEA implementation, just as it does for other national and social programs. The source of this funding could be additional appropriations granted by Congress⁵⁴ or a specific tax imposed on all taxpayers.

If either the government or the general public does not pay for CALEA implementation costs as suggested above and those costs are imposed upon providers, BellSouth and others urge the Commission to allow providers flexibility in how they recover their CALEA implementation costs.⁵⁵ Providers should have the discretion to absorb costs or pass them along to their

⁵³ BellSouth Comments at 42-43; TIA Comments at 22.

⁵⁴ It is both reasonable and fair to consider a general appropriation by Congress to cover carrier CALEA implementation costs. For nearly 100 years, the consumers of communications services have borne the burden of the 3% federal excise tax. This tax has resulted in the collection of billions of dollars from communications' consumers without any corresponding benefit to the industry. Given the significant financial contribution to the Nation's various programs and projects through this federal excise tax, the principles of fundamental fairness and equity weigh strongly in favor of ensuring that communications providers are able to recover their full CALEA implementation costs. BellSouth submits that the most effective way to achieve this objective is through a sufficiently funded Congressional appropriation.

⁵⁵ See, e.g., BellSouth Comments at 43; USTA Comments at 10; Verizon Comments at 26-27.

customers (including law enforcement) through adjusted rates and/or end-user line charges, whichever they choose. CALEA expressly permits such recovery. Section 229(e) grants the Commission authority to allow a carrier to adjust its rates to recover CALEA implementation costs.⁵⁶

VIII. THE COMMISSION SHOULD ALLOW BUT NOT REQUIRE PROVIDERS TO USE TRUSTED THIRD PARTIES TO SATISFY THEIR CALEA OBLIGATIONS.

A significant number of commenters agree that there may be some value in the use of a trusted third party as a means for providers to meet their CALEA obligations. None of these commenters, however, support mandated use of trusted third parties.⁵⁷ Indeed, as the record demonstrates, a number of unanswered questions and legitimate concerns regarding the use of these entities remain (*e.g.*, the privacy and security of communications; who bears the cost responsibility).⁵⁸

BellSouth agrees with commenters such as Nextel and SBC that the mere availability of a trusted third party solution does not make call-identifying information “reasonably available” to a specific carrier.⁵⁹ Indeed, what is “reasonably available” for one carrier through the use of a

⁵⁶ 47 U.S.C. § 229(e).

⁵⁷ *See, e.g.*, BellSouth Comments at 43-44; Cingular Comments at 20; Coalition for Reasonable Rural Broadband CALEA Compliance Comments at 16; Joint Comments of the Industry and Public Interest (Center for Democracy & Technology) at 51; Nextel Comments at 8; SBC Comments at 18-20; TIA Comments at 19-20; T-Mobile USA, Inc. (“T-Mobile”) Comments at 22-23; US ISPA Comments at 27-29; Verizon Comments at 23-24.

⁵⁸ *See, e.g.*, BellSouth Comments at 44; Coalition for Reasonable Rural Broadband CALEA Compliance Comments at 16; Telecom Consulting Associates (“TCA”) Comments at 3; T-Mobile Comments at 22-23.

⁵⁹ *See, e.g.*, Nextel Comments at 8; SBC comments at 19-20; T-Mobile Comments at 22; US ISPA Comments at 29.

trusted third party may not be the same for a different provider with a different network, different engineering needs, and different costs. Carriers, not trusted third parties, have the obligation to meet the assistance capability requirements of CALEA. As such, they must retain the ability to determine the method of complying with CALEA as intended by Congress.

BellSouth also cautions the Commission against accepting the claims and representations of commenters that would serve as trusted third parties without further detailed investigation. As Verizon concludes, “[t]he Commission also should not allow the representations of parties that might act as such Trusted Third parties to shape the Commission’s views of what information meets the statutory ‘reasonably available’ standard, what the proper time frame for CALEA compliance is, or what extensions should be available for carriers who are unable to comply.”⁶⁰

The record demonstrates that concerns about trusted third parties’ willingness to cater exclusively to the demands of law enforcement are legitimate. In its comments, Verisign states that, “[i]f standards do not exist, or are deemed deficient by law enforcement, or are evolving because of changed or additional law enforcement requirements, the service bureau effects necessary interim solutions to the satisfaction of law enforcement and their collection and analysis equipment vendors.”⁶¹ Verisign later repeats a similar statement: “In those instances where the specifications may be deemed ‘deficient’ by law enforcement, the service bureau would supplement those standards to alleviate the deficiency.”⁶² These statements suggest that Verisign is willing to tailor its solutions to the demands of law enforcement without

⁶⁰ Verizon Comments at 25.

⁶¹ Verisign Comments at 21.

⁶² Verisign Comments at 22.

consideration of the existing standards or “safe harbors” or without consultation with the provider in cases where uncertainty may exist regarding what standards apply.

Moreover, Verisign’s statements indicate a fundamental misunderstanding of the CALEA statute itself. CALEA does not authorize law enforcement to dictate standards or unilaterally conclude that standards are deficient. As indicated in Section II. above, Congress charged the industry with developing standards that serve as “safe harbors,” and if a provider complies with these standards, that provider is deemed to have satisfied its CALEA obligations.⁶³ In sum, law enforcement cannot “deem” any specifications or standards deficient. Only the Commission can make such a determination upon the filing of a petition pursuant to Section 1007(b) of CALEA.⁶⁴

As the foregoing demonstrates, there are tangible risks associated with the third party solution. Namely, the incentive by the trusted third party to adopt capabilities beyond those required by CALEA and to pass the costs of those capabilities onto providers. If the Commission sanctions the voluntary use of trusted third parties, it must make clear that these entities are prohibited from adopting ad hoc technical standards simply to meet the demands of law enforcement.

BellSouth also opposes Verisign’s suggestion that the Commission establish a routine CALEA certification process.⁶⁵ As an initial matter, CALEA does not require a continuing certification process. Providers bear the ultimate responsibility for compliance and are subject to enforcement action by the federal courts for their failure to comply. Thus, carriers have a duty and an incentive to comply with CALEA that makes certification unnecessary.

⁶³ See 47 U.S.C. § 1006(a)(1), (2).

⁶⁴ 47 U.S.C. § 1006(b).

⁶⁵ See Verisign Comments at 37-38.

Although it is surely obvious to the Commission, Verisign has a financial self-interest in requiring such a process. If routine certifications were mandated, Verisign would provide the testing services needed in order for a provider to certify its compliance. This business would generate significant revenue for Verisign and other trusted third parties, while simultaneously imposing unnecessary costs and burdens upon the industry. Accordingly, the Commission should reject Verisign's certification proposal.

IX. CONCLUSION

BellSouth remains committed to fulfilling its obligations under CALEA. However, as the record makes clear, many of the proposals set forth in the *Notice* go far beyond the scope of the CALEA statute. The only way to achieve the objectives sought by the Commission is through a statutory amendment to CALEA. In the absence of such an amendment, the Commission must act within the bounds of the law. In order to ensure that any new rules fit within the scope of CALEA, the Commission should take the following actions:

1. Allow industry standards-setting bodies, in consultation with law enforcement, to complete efforts to establish appropriate surveillance standards for broadband services, including determining what requirements are necessary to meet the statutory definition of call-identifying information for broadband transport, Voice Over Internet Protocol ("VoIP") services, and emerging services;
2. Clarify and define the scope of a provider's CALEA obligations based upon the information within that entity's control and which that entity uses in order to provide its CALEA-covered services to its customers;
3. Establish a reasonable process for reviewing petitions seeking relief under Section 109 that does not undermine the protections afforded by Congress;
4. Establish reasonable and realistic deadlines for complying with any new regulations adopted in this proceeding;
5. Recognize that CALEA enforcement lies exclusively with the federal courts and refuse to establish a separate enforcement mechanism;

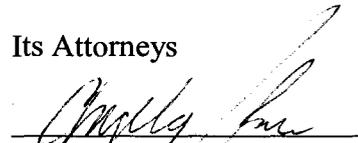
6. Find that the government should be responsible for CALEA implementation costs as CALEA benefits the entire Nation; in the event the Commission declines to adopt this conclusion, it should grant providers flexibility to recover CALEA implementation costs; and
7. Allow for the voluntary use of trusted third parties as a means for providers to satisfy their CALEA obligations subject to certain safeguards.

Respectfully submitted,

BELLSOUTH CORPORATION

Its Attorneys

By:


Angela N. Brown
J. Lloyd Nault, II
675 West Peachtree Street, N. E.
Suite 4300
Atlanta, GA 30375-0001
(404) 335-0724
(404) 335-0737

December 21, 2004

CERTIFICATE OF SERVICE

I do hereby certify that I have this 21st day of December 2004 served the parties of record to this action with a copy of the foregoing **REPLY COMMENTS** by electronic mail and/or by placing a true and correct copy of the same in the United States Mail, postage prepaid, addressed to the parties on the attached service list:


Lynn Barclay

VIA (*) ELECTRONIC MAIL

Service List ET Docket No. 04-295

James X. Dempsey
John B. Morris, Jr.
Lara M. Flint
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006

Douglas Campbell
AMA Techtel Communications, LLC
4909 Canyon Drive
Amarillo, Texas 79110

Christopher R. Calabrese
Barry Steinhardt
American Civil Liberties Union
Technology & Liberty Program
125 Broad Street
17th Floor
New York, NY 10004

Laura W. Murphy
Marvin Johnson
American Civil Liberties Union
Washington Legislative Office
915 15th Street, NW
Washington, DC 20005

Gerard J. Duffy
Coalition for Reasonable Rural
Broadband CALEA Compliance
Blooston, Mordkofsky, Dickens,
Duffy & Prendergast
2120 L Street, NW (Suite 300)
Washington, DC 20037

Donald J. Evans, Esq.
Corr Wireless Communications, L.L.C.
Fletcher, Heald & Hildreth, P.L.C.
1300 North 17th Street, 11th Floor
Arlington, VA 22209

Albert Gidari
CTIA-Wireless Association
Perkins Coie LLP
505 Fifth Avenue South
Suite 620
Seattle, WA 98104

Michael F. Altschul
Cellular Telecommunications and
Internet Association
1400 16th Street, N.W.
Suite 600
Washington, D. C. 20036

Donald Clark Jackson
17720 Vista Avenue
Mote Sereno, CA 95030-3245

John W. Butler
Earl W. Comstock,
Robert K. Magovern
EarthLink, Inc.
Sher & Blackwell LLP
1850 M Street, N. W., Suite 900
Washington, DC 20036

David N. Baker
Vice President for Law
And Public Policy
EarthLink, Inc.
1375 Peachtree Street
Atlanta, Georgia 30309

Albert Gidari
Educause Coalition
Perkins Coie LLP
505 Fifth Avenue South
Suite 620
Seattle, WA 98104

Lee Tien, Esq.
Kurt Opsahl, Esq.
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Susanna M. Zwerling
John Christopher Prather
New York State Attorney
General's Office
120 Broadway
New York, NY 10271

Karl Heinz Rosenbrock
Peter van der Arend
European Telecommunications
Standards Institute
ETSI Secretariat
650, route des Lucioles
06921 Sophia-Antipolis Cedex
FRANCE

H. Michael Warren, President
Douglas J. McCollum, General VP Services
Fiducianet, Inc.
2121 Cooperative Way
Suite 200
Herndon, VA 20171

Paul Kouroupas
Vice President, Regulatory Affairs
Global Crossing North America, Inc.
200 Park Avenue, 3rd Floor
Florham Park, New Jersey 07932

Teresa D. Baer
Jeffrey A. Marks
Global Crossing North American, Inc.
Latham & Watkins, LLP
555 Eleventh Street, N. W., Suite 1000
Washington, D.C. 20004

Jeffrey H. Smith
VP, Western Region Div. Manager
GVNW Consulting, Inc.
PO Box 2330
Tualatin, OR 97062

Stewart A. Baker
Chung Hsiang Mah
Level 3 Communications, LLC
1330 Connecticut Avenue NW
Washington, DC 20036

Greg L. Rogers
Levela 3 Communications, LLC
1025 Eldorado Boulevard
Broomfield, CO 80021

Timothy Harr
Mary Bronner
Motorola, Inc.
1350 I Street NW, Suite 400
Washington, D.C. 2005

Christopher W. Savage
National Cable & Telecommunications
Association
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, DC 20006

Daniel L. Brenner
Neal M. Goldberg
Michael S. Schooler
National Cable & Telecommunications
Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036

Robert H. McNamara
Senior Counsel – Regulatory
Ray Rothermel
Counsel – Regulatory
Nextel Communications, Inc.
2001 Edmund Halley Drive
Reston, VA 20191

L. Marie Guillory
Jill M. Canfield
National Telecommunications
Cooperative Association
4121 Wilson Boulevard, 10th Floor
Arlington, VA 22203

Stuart Polikoff
John McHugh
Stephen Pastorkovich
OPASTCO
21 Dupont Circle, NW
Suite 700
Washington, DC 20036

David L. Nace
Pamela L. Gist
Rural Cellular Association
Lukas, Nace, Gutierrez & Sachs, Chartered
1650 Tyson Boulevard, Suite 1500
McLean, Virginia 22102

Caressa D. Bennet
Marjorie Spivak
Joshua P. Zeldis
Rural Telecommunications
Group, Inc.
Bennet & Bennet, PLLC
10 G Street, NE
Seventh Floor
Washington, DC 20002

Mary Kathryn Kunch
Ron Comingdeer
Kendall W. Parrish
Rural Telecommunications Providers
Comingdeer, Lee & Gooch
6011 N. Robinson
Oklahoma City, OK 73118

Tamber Ray
Rural Telecommunications Providers
The Adams Legal Firm, LLC
1474 North Point Village Center #301
Reston, VA 20294

Christopher F. Miller
MaineStreet Communications, Inc.
208 Portland Road
Gray, ME 04039-9504

Kathleen Wallman
Nuvio Corporation
9332 Ramey Lane
Great Falls, VA 22066-2025

Jennifer Brown
Gary Phillips
Paul K. Mancini
SBC Communicaitons, Inc.
1401 Eye Street, NW
Suite 1100
Washington, DC 20005

David Cavossa
Executive Director
Satellite Industry Association
Suite 600
225 Reinekers Lane
Alexandria, VA 22314

Roger V. Thompson
President
Smithville Telephone Company
Post Office Box 117
63470 Highway 25 North
Smithville, MS 38870

Steve Bock
President
Subsentio, Inc.
1554 E. Easter Circle
Centennial, CO 80122

TCA, Inc-Telecom Consulting Associates
1465 Kelly Johnson Blvd., Suite 200
Colorado Springs, CO 80920

Thomas A. Davis, Jr.
Director
Texas Department of Public Safety
5805 N. Lamar Blvd, Box 4087
Austin, Texas 78773-0001

Matthew J. Flanigan, President
Grant E. Seifreert, Vice President
Derek R. Khlopin, Director
Law and Public Policy
The Telecommunications Industry Assoc.
2500 Wilson Boulevard, Suite 300
Arlington, VA 22201

Thomas J. Sugrue, Vice President
Government Affairs
Robert A. Calaff, Director-Federal Policy
T-Mobile USA, Inc.
401 9th Street, N.W., Suite 550
Washington, DC 20004

Laura H. Parsky
Deputy Assistant Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Suite 2113
Washington, DC 20530

Stewart A. Baker
United States Internet Service
Provider Association
Steptoe & Johnson
1330 Connecticut Avenue, NW
Washington, DC 20036

James W. Olson
Michael T. McMenamin
Robin E. Tuttle
Indra S. Chalk
United States Telecom Association
1401 H Street, NW, Suite 600
Washington, D.C. 20005

Anthony M. Ruthkowski
Vice President for Regulatory Affairs
VeriSign Communicaitons Services Div.
21355 Ridgetop Circle
Dulles, VA 20166-6503

Michael Aisenberg
Director, Government Relations
VeriSign, Inc.
1666 K Street, NW., Suite 410
Washington, D.C. 20006-1227

Brian Cute
Director, Government Relations
VeriSign, Inc.
1666 K Street, N. W., Suite 410
Washington, D.C. 20006

Raj Puri
Vice President, Net Discovery Service
VerSign, Inc.
487 East Middle field Road
Mountain View 94043=4047

Michael E. Glover
Verizon
1515 North Court House Road
Arlington, VA 22201

Karen Zacharia
Joshua E. Swift
Verizon
1515 North Court House Road
Arlington, VA 22201

Smir C. Jain
Meredith B. Halama
Verizon
Wilmer Cutler Pickering Hale
And Dorr LLP
2445 M Street
Washington, DC 20037-1420

John Scheibel
Vice President, Public Policy
Yahoo, Inc.
2000 Pennsylvania Avenue, NW
4th Floor
Washington, DC 20006

John W. Butler
Earl W. Comstock
Robert K. Magovern
Yahoo, Inc.
Sher & Blackwell, LLP
1850 M Street, N.W., Suite 900
Washington, DC 20036

+Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
The Portals, 445 12th Street, S. W.
Room TW-A325
Washington, D.C. 20554

+Best Copy and Printing, Inc.
The Portals, 445 12th Street, S.W.
Room CY-B402
Washington, D.C. 20554

+ VIA ELECTRONIC FILING