

**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

COMMENTS

BELLSOUTH CORPORATION

Angela N. Brown
J. Lloyd Nault, II

Its Attorneys

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

November 8, 2004

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	1
II.	BROADBAND INTERNET ACCESS PROVIDERS ARE EXEMPT FROM CALEA UNDER THE INFORMATION SERVICES EXCLUSION.	5
III.	THE COMMISSION MUST CONSIDER CAREFULLY ANY DETERMINATION MADE UNDER THE “SUBSTANTIAL REPLACEMENT” STANDARD.	12
IV.	THE INDUSTRY SHOULD CONTINUE TO WORK WITH LAW ENFORCEMENT TO DEVELOP CALEA STANDARDS AS INTENDED BY CONGRESS.....	15
V.	THE SCOPE OF A PROVIDER’S CALEA OBLIGATIONS VARIES WITH THE TYPE OF SERVICE AT ISSUE.	19
	A. The Commission Should More Clearly Define the Phrase “Reasonably Available” in Order to Identify a Carrier’s Obligation to Provide Call-Identifying Information.....	20
	B. Call-Identifying Information for Circuit-Switched Services and Broadband Services Is Not the Same.....	23
VI.	THE COMMISSION SHOULD NOT ADOPT LAW ENFORCEMENT’S PROPOSED FRAMEWORK FOR BENCHMARKS, COMPLIANCE DEADLINES, AND EXTENSIONS.....	28
	A. BellSouth Supports a Blanket Extension for Packet-Mode Communications.....	29
	B. The Commission Should Modify Its Proposed Framework for Considering Section 109(b) Petitions.....	30
	C. The Commission Should Not Establish Benchmarks and Interim Deadlines.	33
VII.	CALEA ENFORCEMENT LIES EXCLUSIVELY WITH THE FEDERAL COURTS..	38
VIII.	ANY CALEA RULES ADOPTED BY THE COMMISSION MUST NOT STIFLE INNOVATION.	40
IX.	REQUIRING PROVIDERS TO BEAR THE SOLE RESPONSIBILITY FOR CALEA IMPLEMENTATION COSTS IS INCONSISTENT WITH CALEA.	42

X. THE COMMISSION SHOULD ALLOW BUT NOT REQUIRE PROVIDERS TO USE TRUSTED THIRD PARTIES TO SATISFY THEIR CALEA OBLIGATIONS.....43

XI. CONCLUSION.....45

**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

COMMENTS

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

I. INTRODUCTION AND SUMMARY

BellSouth supports the development of a balanced approach to ensuring compliance with the Communications Assistance for Law Enforcement Act (“CALEA”) as intended by Congress. Specifically, any approach adopted by the Commission must ensure that the needs of law enforcement are met, while simultaneously protecting privacy and not impeding technological innovation as required by the statute and its legislative history. A number of the tentative conclusions and proposals set forth in the *Notice*, however, fail to satisfy this standard.

The positions expressed herein are not an attempt to limit law enforcement efforts at a

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*, DA 04-187 (rel. Aug. 9, 2004) (“*Notice*”).

time of heightened national security concerns. The goal, rather, is to achieve a solution that is legally sustainable so that the industry can move forward with creating new and innovative technologies in cooperation with law enforcement instead of proceeding down a path of protracted litigation. Moreover, national security concerns should not and cannot be used as a veil for the Commission to embark upon an administrative re-write of CALEA when the statute does not grant such authority. The Commission is obligated to implement CALEA as enacted into law by Congress, yet many of the rules and requirements proposed in the *Notice* are plainly inconsistent with both the language and legislative history of the statute. However laudable the results sought by the Commission and law enforcement may be, they are simply not permitted under CALEA.

Trying to extend the scope of CALEA and the Commission's authority thereunder in contravention of the statute will not lead to solutions that will protect public safety. To the contrary, the legal deficiencies of the proposals, if adopted, make them susceptible to court challenges that will only lengthen the time in which law enforcement and the industry are left without answers. 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 amendments, however, the Commission is obligated to act within the confines of the current statute.

Given CALEA's statutory constraints, the Commission's inquiry should begin with a clear understanding of exactly what law enforcement is seeking, how carriers are allegedly not meeting the government's needs,² and what information carriers are able to provide law

² Law enforcement's allegations of carriers' failure to cooperate and comply with CALEA have not been substantiated with any documented evidence. In a recent audit of the Department of Justice, the federal auditor stated: "[T]he FBI was unable to provide [the Auditor] with data

enforcement today. As demonstrated more fully below, besides the legal infirmities of applying CALEA to broadband access and Internet service providers as recommended in the *Notice*, such an approach may not be the most effective, cost-efficient, and timely method of meeting law enforcement's needs. Indeed, if the true goal of law enforcement is to use electronic surveillance to fight crime and terrorism expeditiously, the government should work collaboratively with the industry to develop tailored solutions within the boundaries of the current law.

Many of those solutions already exist and are used effectively by law enforcement today. All providers (including information service providers) are statutorily obligated to assist the government in conducting lawfully authorized electronic surveillance under long-standing statutes (*e.g.*, the Omnibus Crime Control and Safe Streets Act of 1968; the Electronic Communications Privacy Act;³ the pen register and trap and trace statute⁴). CALEA does not replace or supersede these general wiretap laws, but, rather, supplements them. Thus, should the Commission decline to adopt the proposals endorsed by law enforcement, federal and local agencies will still have available to them the means to conduct lawfully authorized electronic surveillance.

Moreover, the industry in general and BellSouth in particular have a long history of cooperation with law enforcement under the general electronic surveillance laws identified above

showing the extent to which state and local law enforcement has been unable to conduct electronic surveillance as a result of these delays [in implementing CALEA solutions.]” 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 6 (April 2004).

³ 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.).

⁴ 18 U.S.C. §§ 3121 *et seq.*

as well as CALEA, and this cooperation continues to date. For example, throughout the last several years, consistent with its obligations, BellSouth has spent millions of dollars upgrading its equipment to deploy CALEA-compliant solutions, where available, in order to satisfy the core assistance capability requirements of CALEA, the “punch list” requirements, and the requirements for packet-mode communications. In addition, Internet service providers, including BellSouth, though expressly exempt from CALEA, have executed surveillances requested by law enforcement under the general wiretap laws. The industry’s long-standing cooperation with law enforcement therefore should not be dismissed or minimized. In fact, it should be recognized that law enforcement has the existing authority to obtain court orders for the surveillance of broadband services that are the subject of this *Notice*. Further, law enforcement has used – and continues to use – this authority to conduct lawful intercepts on broadband services that are outside the scope of CALEA. In other words, CALEA is by no means the only way for law enforcement to protect the national security.

Thus, rather than unlawfully expanding the scope of CALEA as proposed in the *Notice*, the Commission should allow the industry, working together with law enforcement, to develop the most effective and cost-efficient methods for meeting the electronic surveillance needs of the government. BellSouth therefore urges the Commission to take the following actions:

1. Adhere to the law by concluding that broadband Internet access providers are information service providers that are exempt from the requirements of CALEA;
2. Establish an analytical framework that considers market conditions in order to determine whether a particular service meets the “substantial replacement” standard of CALEA and is therefore subject to the statute’s assistance capability requirements;
3. Allow industry standards-setting bodies, in consultation with law enforcement, to complete efforts to establish appropriate standards governing packet-mode communications, including determining what information meets the statutory

definition of call-identifying information for broadband transport, Voice Over Internet Protocol (“VoIP”) services, and emerging services;

4. 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;
5. Continue to decline to adopt law enforcement’s proposed framework for CALEA benchmarks and deadlines;
6. Grant a blanket extension for packet-mode communications applicable to the entire industry upon adoption of a final order in this proceeding;
7. Recognize that CALEA enforcement lies exclusively with the federal courts and refuse to establish a separate enforcement mechanism;
8. Continue to decline to adopt law enforcement’s proposals regarding the identification of future services and entities subject to CALEA;
9. 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
10. Allow for the voluntary use of trusted third parties as a means for providers to satisfy their CALEA obligations.

II. BROADBAND INTERNET ACCESS PROVIDERS ARE EXEMPT FROM CALEA UNDER THE INFORMATION SERVICES EXCLUSION.

The Commission’s proposed definition of “broadband access service” attempts to sweep within the scope of CALEA those providers offering integrated Internet access service over their own facilities. Such an outcome is not only inconsistent with CALEA but also unnecessary. As an initial matter, it is important to note that the information services exclusion does not relieve broadband Internet access providers or other information service providers of their statutory obligations to assist law enforcement in conducting lawfully authorized wiretaps. Therefore,

there is no need to adopt overly expansive (and unlawful) interpretations of CALEA as proposed in the *Notice*, even assuming it were lawful for the Commission to do so (which is not the case).

Contrary to the Commission's proposed findings, CALEA applies to a limited set of telecommunications services and providers. Specifically, CALEA applies only to "telecommunications carriers," which Section 1001(8)(A) defines as entities "engaged in the transmission or switching of wire or electronic communications as [] common carrier[s] for hire."⁵ In addition, the legislative history states, "[t]he only entities required to comply with the functional requirements [of CALEA] are telecommunications common carriers."⁶ Expressly exempted from CALEA are information services,⁷ private carrier telecommunications,⁸ and interconnection services and facilities.⁹

Notwithstanding the plain language of the statute and its legislative history, the Commission eviscerates these distinctions by tentatively concluding that facilities-based providers of any type of broadband Internet access service¹⁰ are subject to CALEA. The

⁵ 47 U.S.C. § 1001(8)(A).

⁶ H.R. Rep. No. 103-827 at 18 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3498 ("H.R. Rep.").

⁷ 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A).

⁸ *Id.* § 1002(b)(2)(B).

⁹ *Id.*

¹⁰ The Commission relies upon the definition of "broadband access service" originally proposed by the Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration – "the process and service used to gain access or connect to the public Internet using a connection based on packet-mode technology that offers high bandwidth. The term is intended to be inclusive of services that the Commission has previously defined as 'wireline broadband Internet access' and 'cable modem service' as well as other services providing the same function through different technology, such as wireless technology. The term does not include any 'information services' available to a user after he or she has been connected to the Internet, such as the content found on Internet Service Providers' or other websites. 'Broadband access services' includes the platforms currently used to achieve broadband connectivity (*e.g.*, wireline, cable modem, wireless, fixed wireless, satellite, and broadband access over power line) as well as any platforms that may in the future be used to achieve broadband connectivity."

Commission bases its conclusion upon differences between the definitions of “telecommunications carrier” in the CALEA statute and the Communications Act. Specifically, the Commission finds that broadband Internet access is “a replacement for a substantial portion of the local telephone exchange service used for dial-up Internet access service and treating such providers as telecommunications carriers for purposes of CALEA is in the public interest.”¹¹ This finding is much broader than Congress intended as it subjects information service providers to CALEA’s requirements in direct contravention of the statute. Accordingly, the Commission’s tentative conclusion is legally unsupportable.

Definitional nuances do not transform information services into telecommunications services. As the Commission has previously found, “Internet access service is appropriately classified as an information service, because the provider offers a single, integrated service, Internet access, to the subscriber.”¹² The Commission further found that Internet access service goes beyond the provision of a “transparent transmission path to offer end users the ‘capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information.’”¹³

Notice, ¶ 32 (citing Joint Petition for Expedited Rulemaking, RM-10865, at 15-16 (filed Mar. 10, 2004) (“Joint Petition”)).

¹¹ *Notice*, ¶ 37.

¹² *Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, GN Docket No. 00-185 & CS Docket No. 02-52, *Declaratory Ruling and Notice of Proposed Rulemaking*, 17 FCC Rcd 4798, 4821, ¶ 36 (2002) (“*Cable Modem Declaratory Ruling*”), citing *Federal-State Joint Board on Universal Service*, CC Docket No. 96-45, *Report to Congress*, 13 FCC Rcd 11501, 11536, ¶ 73 (1998) (“*Universal Service Report*”) (emphasis added).

¹³ *Universal Service Report*, 13 FCC Rcd at 11536, ¶ 74 (citing 47 U.S.C. § 153(20)).

The Commission seeks to distance itself from these previous findings by relying on differences between the definitions of “telecommunications carrier” in the CALEA statute and the Communications Act. It is certainly true that CALEA allows the Commission to classify an entity as a telecommunications carrier for CALEA purposes, if the Commission finds that the service provided by that entity “is a replacement for a substantial portion of the local telephone exchange service” and such a designation will serve the public interest.¹⁴ However, the idea that broadband Internet access satisfies this statutory standard because it replaces a single functionality of local telephone exchange service – dial-up Internet access – is flawed and wholly inconsistent with the functionality of the service. Commissioner Michael J. Copps acknowledged as much:

To me, it strains credibility to suggest that Congress intended “a replacement for a substantial portion of the local telephone exchange” to mean the replacement of *any* portion of any individual subscriber’s functionality.¹⁵

To be considered, for the purposes of CALEA, “a replacement for a substantial portion of the local exchange service,” a service must be capable of replacing all (or at least a majority) of the functionalities of local exchange service, including, for example, the ability to make local voice calls, access to 911, and access to long distance service. Dial-up Internet access is a single feature of local exchange service and is used almost exclusively to reach information services that are not subject to CALEA. Defining broadband Internet access as within the scope of CALEA because it replaces a single, finite capability of local exchange service would be a

¹⁴ 47 U.S.C. 1001(8)(B)(ii).

¹⁵ *Notice*, Statement of Commissioner Michael J. Copps, Concurring (emphasis included in original).

complete misreading of the statute and is not necessary in order for law enforcement to continue to obtain the electronic surveillance assistance it needs.

Furthermore, whether or not broadband Internet access service is “a replacement for a substantial portion of the local telephone exchange service,” Internet access service providers are exempt from CALEA under the plain language of the statute. CALEA expressly excludes from coverage “all information services, such as Internet service providers or services such as Prodigy and America-On-Line.”¹⁶ Although the Commission seeks to include Internet access providers under the definition of “telecommunications carrier” by broadly defining the term “switching” in Section 1001(8), the fact that Internet access uses a switching functionality does not magically transform an information service that is exempt from CALEA into a telecommunications service that is subject to CALEA.

Moreover, despite the Commission’s purported focus on statutory definitions and distinctions, it pays little attention to the fact that CALEA’s definition of “information services” is nearly identical to that contained in the Communications Act. Section 153(20) of the Communications Act defines an “information service” as:

the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.¹⁷

Using essentially the same verbiage, organized slightly differently, Congress defines the term “information service” in CALEA as:

¹⁶ H.R. Rep. at 18, 1994 U.S.C.C.A.N. at 3498; *see* 47 U.S.C. § 1001(8)(C) (“The term “telecommunications carrier”—(C) does not include—(i) persons or entities insofar as they are engaged in providing information services.”).

¹⁷ 47 U.S.C. § 153(20).

- (A) [T]he offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and
- (B) includes—
 - (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;
 - (ii) electronic publishing; and
 - (iii) electronic messaging services; but
- (C) does not include any capability for a telecommunications carrier’s internal management, control, or operation of its telecommunications network.¹⁸

The overwhelming similarities between these two definitions suggest that, if a service is deemed to be an “information service” under the Communications Act, it also must be classified as an “information service” under CALEA. As demonstrated above, the Commission has already concluded that Internet access is an “information service” under the Communications Act; therefore, Internet access must necessarily qualify as an “information service” under CALEA and therefore is exempt from any CALEA obligations. Neither the “substantial replacement” provision nor an overly expansive definition of the term “telecommunications carrier” can trump the information services exemption.

Moreover, the Commission’s assertion that Internet access services/information services meet CALEA’s “substantial replacement” standard as telecommunications services subject to CALEA¹⁹ ignores the principles of statutory construction. The information services exclusion follows CALEA’s “substantial replacement” provision in the definition of a “telecommunications carrier” and includes an unambiguous and clearly stated exception. The use of the phrase “but does not include” at the conclusion of the “substantial replacement”

¹⁸ *Id.* § 1001(6).

¹⁹ *Notice*, ¶ 50.

provision is a clear indication that Congress did not intend the “substantial replacement” standard to trump the information services exemption. Section 1008 expressly states that the term “telecommunications carrier” “does not include persons or entities insofar as they are engaged in providing information services.”²⁰ Thus, a finding by the Commission that an entity is a telecommunications carrier, for purposes of CALEA, under the substantial replacement provision does not subject that entity to CALEA if that entity is engaged in the provision of information services, which includes Internet access.

In addition, the use of the negative or exclusionary word “not” is further persuasive evidence that the statutory prohibition against subjecting information service providers to CALEA is mandatory.²¹ Section 1001(8) has three distinct subsections. The first section defines a “telecommunications carrier” as “a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire.” The second section expands upon the first by stating that telecommunications carriers include: (1) CMRS providers and (2) persons or entities that provide a service found by the Commission to be a replacement for a substantial portion of the local telephone exchange service. Finally, the third section describes those entities that are expressly exempt from the definition of a “telecommunications carrier” as defined in the preceding two subsections. The rules of statutory construction simply do not permit the Commission to negate the information services exemption as the *Notice* proposes. Indeed, the Commission’s authority to designate entities as “telecommunications carriers” pursuant to Section 1001(8)(B)(ii) does not eliminate or trump this statutory exemption.

²⁰ 47 U.S.C. § 1001(8)(C)(i).

²¹ See 2B Norman J. Singer, Sutherland Statutes and Statutory Construction, § 57:9 (6th ed. Feb. 2004) (“Sutherland”).

Despite the exemption of information service providers from compliance with CALEA, these entities are not excused from their obligation to assist law enforcement in conducting lawfully authorized electronic surveillance pursuant to traditional wiretap laws. As Congress pointed out, “information services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the capability requirements”²² of CALEA. Thus, law enforcement still can obtain the information it needs from providers of information services without subjecting these entities to CALEA.

III. THE COMMISSION MUST CONSIDER CAREFULLY ANY DETERMINATION MADE UNDER THE “SUBSTANTIAL REPLACEMENT” STANDARD.

The Commission must establish a legally sustainable framework for considering whether an entity qualifies as a “telecommunications carrier” subject to CALEA under the “substantial replacement” provision of Section 1001(8)(B)(ii). Under this statutory provision, if “any person or entity engaged in providing wire or electronic communications or switching service” is providing “a replacement for a substantial portion of the local exchange service,” the Commission may classify such a person or entity as a telecommunications carrier subject to CALEA.²³ Congress directed the Commission to consider the extent to which an entity’s service is “a replacement for the local telephone service to a *substantial portion of the public within a*

²² H.R. Rep. at 18, 1994 U.S.C.C.A.N. at 3498. The Commission itself has pointed out that, “while CALEA excludes providers of information services from the requirement that they modify their networks in accordance with regulations promulgated by the Attorney General, CALEA does not exclude providers of information services from the duty to provide law enforcement personnel with interceptions in response to a court order.” *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Notice of Proposed Rulemaking*, 13 FCC Rcd 3149, 3159, ¶ 13 (1997) (emphasis added).

²³ 47 U.S.C. § 1001(8)(B)(ii).

state,”²⁴ when the Commission determines whether a service should be made subject to the requirements of CALEA. Thus, the answer to the Commission’s query in a footnote as to whether the phrase “within a state” “has any material significance to [its] determination of whether a service is a substantial local exchange replacement”²⁵ is unequivocally “yes.” Of course, this phrase is relevant because it is part of the legislative history and clearly reflects the intent of Congress. Moreover, as previously stated, CALEA compliance for any such provider’s service is further modified by the information services exclusion set forth in Section 1001(8)(B)(ii).

The Commission has relegated to a footnote its request for comment on other meanings of the “substantial replacement” provision.²⁶ Specifically, in footnote 113, the Commission rejects a prior recommendation to construe the phrase “substantial portion” in Section 1001(8)(B)(ii) in the same way the Commission interpreted the phrase in the context of the definition of commercial mobile service under Section 332(d)(1).²⁷ Section 332(d)(1) defines the term “commercial mobile service” as:

any mobile service . . . that is provided for profit and makes interconnected service available (A) to the public or (B) to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Commission.”²⁸

The Commission dismisses the language in Section 332 as a source of guidance based upon the fact that the language in the two statutes (though similar) is different.²⁹ Such an

²⁴ H.R. Rep. at 20-21, 1994 U.S.C.C.A.N. at 3500-01 (emphasis added).

²⁵ *Notice*, n.106.

²⁶ *Id.*, n.113.

²⁷ *Id.*

²⁸ 47 U.S.C. § 332(d)(1) (emphasis added).

²⁹ *Notice*, n.113.

approach is completely inconsistent with the statutory principle of interpreting one statute by analogy or reference to similar language in another statute.³⁰

The Commission also fails to consider similar “substantial replacement” language in another statutory provision, Section 332(c), as a tool for interpreting properly the CALEA substantial replacement provision.³¹ Section 332(c)(3)(A) authorizes the Commission to grant a state permission to regulate the rates for a CMRS service, if the state demonstrates that the CMRS service “is a replacement for land line telephone exchange services for a substantial portion of the telephone land line exchange service within such state.”³² The Commission has found that the mere showing that a CMRS carrier is providing a substitute for landline service is not sufficient to support LEC regulation.³³ The Commission did not interpret the language in Section 332 to mean that a state could regulate CMRS carriers if CMRS service replaced a single functionality of telephone land line exchange service. Rather, there must be a more substantive and quantitative showing as described below.

In considering whether a state should be granted authority to regulate CMRS service, no alternatives for obtaining basic telephone service must exist.³⁴ The types of evidence that the Commission will consider include, among other things:

³⁰ See *Sutherland*, §§ 53:3, 53:4; *Overstreet v. North Shore Corp.*, 318 U.S. 125, 131-32 (1943); *Hecht v. Malley*, 265 U.S. 144, 153 (1924); *United States v. Freeling*, 31 F.R.D. 540, 549 (S.D.N.Y. 1962); *Cooke v. Kilgore Mfg. Co.*, 15 F.R.D. 465, 468 (N.D. Ohio 1954).

³¹ *Notice*, n.113.

³² 47 U.S.C. § 332(c)(3)(ii).

³³ *Petition of the State Independent Alliance and the Independent Telecommunications Group for a Declaratory Ruling that the Basic Universal Service Offering Provided by Western Wireless in Kansas is Subject to Regulation as Local Exchange Service*, WT Docket No. 00-239, *Memorandum Opinion and Order*, 17 FCC Rcd 14802, 14815, n.98 (2002).

³⁴ *Id.*

- (1) the number of CMRS providers in the state; the types of services offered by CMRS providers in the state; and the period of time that these providers have offered service in the state;
- (2) the number of customers of each CMRS provider in the state; trends in each provider's customer base during the most recent annual period; annual revenues and rates of return for each CMRS provider;
- (3) rate information for each CMRS provider, including trends in each provider's rates;
- (4) an assessment of the extent to which services offered by the CMRS providers are substitutable for services offered by other carriers in the state; and
- (5) opportunities for new providers to enter into the provision of competing services, and an analysis of any barriers to entry.³⁵

The Commission could establish a similar analytical framework to determine whether, under CALEA, a service is a replacement for a substantial portion of the local exchange service. A review of market conditions (*e.g.*, number of providers of the particular service at issue, rates charged by these providers, number of customers, etc.) is a more reasonable and statutorily sound approach than that proposed in the *Notice*.

IV. THE INDUSTRY SHOULD CONTINUE TO WORK WITH LAW ENFORCEMENT TO DEVELOP CALEA STANDARDS AS INTENDED BY CONGRESS.

The Commission appropriately recognizes that “[p]acket technologies are fundamentally different from the circuit switched technologies that were the primary focus of the Commission’s earlier decisions.”³⁶ As a result, call-identifying information in the broadband world is not

³⁵ 47 C.F.R. § 20.13(a)(2).

³⁶ *Notice*, ¶ 63.

synonymous with call-identifying information in the circuit-switched world. While BellSouth believes that additional work is necessary to determine what information meets the statutory definition of call-identifying information for broadband transport, Internet access, and VoIP service, the Commission is not the appropriate entity to provide such guidance. The Commission cannot reasonably anticipate the various technologies and define appropriate standards for the entire industry as part of a rulemaking proceeding. Moreover, there is no reason for the Commission to attempt to do so when CALEA gives the industry, through industry associations or standards-setting bodies, the initial responsibility of developing technical standards to implement the requirements of the statute. The statute “provides that the telecommunications industry itself shall decide how to implement law enforcement’s requirements.”³⁷ Congress found it imperative to ensure that “those whose competitive future depends on innovation w[ould] have a key role in interpreting the legislated requirements in finding ways to meet them without impeding the deployment of new services.”³⁸ Thus, standards-setting bodies are the appropriate forums to address the question of what constitutes call-identifying information for packet-based technologies.

No one disputes that the development of CALEA-compliant solutions for the broad array of packet-mode communications offered today is a complicated and time-consuming process. However, progress has been, and continues to be, made. Appropriately, the industry, together with law enforcement, has been working with standard-setting groups to develop technical standards and specifications for packet-mode communications. The activities described below

³⁷ H.R. Rep. at 19, 1994 U.S.C.C.A.N. at 3499.

³⁸ *Id.*

demonstrate that CALEA is working as Congress intended with respect to the development of technical standards.

As background, in December 2000, the initial version of standard ANSI-J-STD-025 (“J-Standard”) was published. This standard provided support for the surveillance of basic voice calls and certain packet-mode communications.³⁹ As the Commission notes, a revision of the J-Standard – ANSI-J-STD-025-B – was approved as a Telecommunications Industry Standard (“TIA”) and an Alliance for Telecommunications Industry Solutions (“ATIS”) trial use standard in January 2004.⁴⁰ This new version of the J-Standard provides enhancements to further support electronic surveillance of packet-data telecommunication services.⁴¹ In January 2004, ANSI also approved ATIS standard T1.724-2004, which supports the surveillance of both Internet access services and session initiation protocol (“SIP”)-based multimedia (including voice) over packets. Standards also have been developed to support the surveillance of VoIP arrangements.⁴²

In addition to the work completed above, a number of new standards projects are underway. For example, version 2 of ANSI T1.678-2004 (a standard for voice-over-packet services)⁴³ is currently being developed in an ATIS committee. This version would expand

³⁹ The J-Standard was modified subsequently to include additional capabilities in order to comply with the Commission’s April 2002 *Order on Remand. Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Order on Remand*, 17 FCC Rcd 6896 (2002). This version modified the definition of what is “reasonably available” and added support for many of the “punch-list” items as required by the Commission.

⁴⁰ *Notice*, Appendix D at 91.

⁴¹ For a detailed discussion of the enhancements, *see Notice*, Appendix D at 91-92.

⁴² *Notice*, Appendix D at 92. In January 2004, ANSI approved ATIS standard T1.678-2004, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks* (ANSI T1.678). This standard supports surveillance of VoIP arrangements using two-call set-up protocols: SIP and H.323-based VoIP services.

⁴³ *Id.*

beyond basic calls and provide support for supplementary services (*e.g.*, call forwarding, call waiting, etc). 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 potentially could offer some new capabilities. This version, in addition to updates and improvements to version B, would provide additional support for packet-data capabilities of wireless technologies. The projected completion date is March 2005.

Law enforcement has been actively involved in the standards-setting process for packet-mode communications. For example, in September 2003, the FBI CALEA implementation unit issued a document entitled “Electronic Surveillance Needs for Public IP Network Access Service (PIPNAS).” This document identified surveillance events related to access to the Internet and listed information elements that law enforcement would like to receive when an event occurs. Based on a proposal by law enforcement, a project is underway in the Packet Technologies and Systems Committee (“PTSC”) group of ATIS to develop a standard to provide electronic surveillance support for public Internet Protocol (“IP”) network access service. The proposed completion date for development of this standard is July 2005.

Much of the information identified by law enforcement in the PIPNAS document is applicable to providers of information services. From the perspective of the entity providing the broadband transport service, access to information similar to call-identifying information in the circuit-switched world is very limited (*i.e.*, most of the detail that law enforcement desires is in the content carried over the transport and is not reasonably available to the transport provider). If law enforcement desires to obtain call-identifying information from a provider of broadband transport service, the only method that is “reasonably achievable” is the delivery of that

provider's entire bit stream. Under this approach, law enforcement can obtain all the call-identifying information it seeks.

As demonstrated above, much work has been done by the industry and standards-setting groups to identify services subject to CALEA and to standardize the development and delivery of CALEA functionality. Law enforcement has played an important role in this process and has provided significant input. Consistent with CALEA, the industry has assumed the lead role in establishing technical requirements that serve as a "safe harbor" for packet-mode communications. Therefore, any claims that the standards-process is failing are disingenuous and not supported by the facts. Indeed, revised J-Standard (J-STD-025-B), adopted by both TIA and ATIS, serves as a "safe harbor" for CALEA compliance.⁴⁴ Therefore, providers such as BellSouth whose networks support this standard are deemed to be in compliance with the assistance capability requirements of CALEA pursuant to Section 1006(a)(2).

Thus, the Commission need only provide clarification or adopt standards if an entity claims that standards either do not exist or are deficient, and files a petition with the Commission as required by Section 1006(b) of CALEA. Neither law enforcement nor any other entity has submitted such a petition; therefore, the Commission is not authorized at this time to establish technical requirements or to define what constitutes call-identifying information for emerging broadband services.

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

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

⁴⁴ *Notice*, Appendix D at 92.

Commission must take these differences into account when determining the scope of a provider's CALEA obligations. Indeed, the Commission should define a provider's obligations under CALEA based upon the information that is both within that entity's control and is utilized by the provider to offer its CALEA-covered services to its end users. This approach is fully consistent with CALEA's legislative history. As Congress 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.⁴⁵

Thus, Congress clearly recognized that there would be instances in which one carrier would not have 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.

A. The Commission Should More Clearly Define the Phrase "Reasonably Available" in Order to Identify a Carrier's Obligation to Provide Call-Identifying Information.

The Commission should find that call-identifying information is "reasonably available" to a provider only if that provider has reasonable access to and uses the information in the provision of its CALEA-covered service to its customers. CALEA defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber, by means of any

⁴⁵ H.R. Rep. at 22, 1994 U.S.C.C.A.N. at 3502.

equipment, facility, or service of a telecommunications carrier.”⁴⁶ CALEA requires a carrier to satisfy the statute’s assistance capability requirements by providing access to call-identifying information “that is reasonably available to the carrier.”⁴⁷

The Commission previously defined the phrase “reasonably available” in its *Third Report and Order* when it found that “[c]all identifying-information is ‘reasonably available’ to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications.”⁴⁸ The Commission later concluded that the term “reasonably” was a qualifier. It stated that “if information is only accessible by significantly modifying a network,” then it is not reasonably available.⁴⁹ In the instant *Notice*, the Commission proposes to apply its prior definition of “reasonably available” to “broadband access” and VoIP services.

Both approaches have the problem of defining “reasonably available” with broad, subjective terms (*e.g.*, “unduly burdened;” “significantly modifying”). Either definition requires an analysis of the specific technology or service at issue and a determination of what information is “reasonably available.” Thus, a more reasonable interpretation of the phrase “reasonably available” is that CALEA requires a provider to deliver call-identifying information only if that provider has reasonable access to the information and uses such information in the provision of its CALEA-covered service to its customers. BellSouth, for example, as a broadband transport

⁴⁶ 47 U.S.C. § 1001(2).

⁴⁷ *Id.* § 1002(a)(2).

⁴⁸ *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Third Report and Order*, 14 FCC Rcd 16794, 16860, Appendix A (1999).

⁴⁹ *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Order on Remand*, 17 FCC Rcd 6896, 6927, ¶ 80 (2002).

provider does not have reasonable access to, and does not utilize or collect, the underlying information contained in the various layers of a packet stream in order to provide transport service; therefore, information other than the full packet stream is not “reasonably available” to it.

In determining “reasonable availability,” the Commission also states that it will not consider cost as a factor.⁵⁰ The complete dismissal of cost as a consideration is wholly inconsistent with the letter and spirit of CALEA. Cost considerations are woven throughout the statute. For example, under Section 1006(b), if standards are found to be absent or deficient, the Commission is authorized to establish technical requirements that, among other things, “meet the assistance capability requirements . . . by cost-effective methods”⁵¹ and “minimize the cost of such compliance on residential ratepayers.”⁵²

In addition, Section 1008(b) allows a carrier to petition the Commission to find that compliance with CALEA is not reasonably achievable for equipment, facilities, or services deployed after January 1, 1995.⁵³ In making its determination, the Commission must consider “whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier’s systems.”⁵⁴ Other factors to be considered include the effect on rates for basic residential telephone services and the need to achieve the capability assistance requirements by cost-effective methods.⁵⁵ Indeed, as Congress explained, “[o]ne factor to be

⁵⁰ *Notice*, ¶ 67.

⁵¹ 47 U.S.C. § 1006(b)(1) (emphasis added).

⁵² *Id.* § 1006(b)(3) (emphasis added).

⁵³ *Id.* § 1008(b).

⁵⁴ *Id.* (emphasis added).

⁵⁵ *Id.* (emphasis added).

considered when determining whether compliance is reasonable is the cost to the carrier of compliance compared to the carrier's overall cost of developing or acquiring and deploying the feature or service in question."⁵⁶ Thus, adopting compliance requirements without regard to cost is impermissible under CALEA. Congress explicitly directs the Commission to consider reasonable achievability, costs, cost-effective methods, and the impact on ratepayers when promulgating CALEA requirements.

B. Call-Identifying Information for Circuit-Switched Services and Broadband Services Is Not the Same.

As the Commission has recognized, "[p]acket technologies are fundamentally different from the circuit-switched technologies that were the primary focus of the Commission's earlier decisions."⁵⁷ As a result, call-identifying information in the broadband world is not synonymous with call-identifying information in the circuit-switched world. The application of CALEA's definition of call-identifying information to broadband services yields very different results than when applied to circuit-based services.

The *Notice* seeks comment on where content and various kinds of call-identifying information are available in the network for packet services and whether the information is "reasonably available" to the provider.⁵⁸ The Commission "anticipate[s] that some call-identifying information may be available from either a VoIP provider or a broadband access

⁵⁶ H.R. Rep. at 19, 1994 U.S.C.C.A.N. at 3499.

⁵⁷ *Notice*, ¶ 63.

⁵⁸ *Id.*, ¶ 68.

provider.”⁵⁹ Further, it asks whether in these instances, call-identifying information would be available from one entity but not the other.⁶⁰

The *Notice* identifies the following as information that law enforcement potentially may seek from a provider of “broadband access” service:

- (1) information about the subject’s access sessions, including start and end times and assigned IP addresses, for both mobile and fixed access sessions;
- (2) information about changes to the subject’s service or account profile, which could include, for example, new or changed logins and passwords; and
- (3) information about packets sent and received by the subject, including source and destination IP addresses, information related to the detection and control of packet transfer security such as those in Virtual Private Networks (“VPNs”), as well as packet filtering to favor certain traffic going to or from certain customers.⁶¹

As stated earlier, the ability to access the various types of information contained in a single communication varies from provider to provider depending upon the type of service offered. For example, BellSouth provides underlying broadband transport service (*e.g.*, DSL) on a wholesale basis to various application/Internet service providers, which, in turn, may offer VoIP services or access to the Internet via passwords to their respective end users. From BellSouth’s perspective as the underlying broadband transport service provider, access to information similar to the call-identifying information for circuit-based communications is very limited, regardless of whether the wholesale customer is providing retail Internet access service or VoIP service. In other words, most of the detail that law enforcement desires resides in the content carried over the transport and is not reasonably available to the transport provider.

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Id.*, ¶ 66.

If law enforcement wants to obtain call-identifying “like” information from a provider of broadband transport service, the only method that is “reasonably achievable” is the delivery of the entire bit stream 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 its switches are not able to process or interpret higher layers of information. Indeed, the broadband transport provider is unaware of even the type of traffic (*e.g.*, voice, data, content, signaling) being transmitted over its facilities.

Limitations on the information that must be supplied to law enforcement and in what form clearly is supported by CALEA’s legislative history. According to Congress, “[i]f the communication at the point it is intercepted is digital, the carrier may provide the signal to law enforcement in digital form. Law enforcement is responsible for determining if a communication is voice, fax or data and for translating it into useable form.”⁶² Thus, CALEA would require a broadband transport provider to provide nothing more than a full packet stream; it would not obligate the carrier to break open the packet for analysis and to provide disaggregated data to law enforcement.

As discussed more fully below, the categories of potential call-identifying information identified by the Commission are either not available at all or would require significant modification of the underlying architecture used to offer transport service. BellSouth examines these categories below:

1. ***Information about the subject’s access sessions, including start and end times and assigned IP addresses, for both mobile and fixed access sessions.*** BellSouth as a provider of broadband transport for Internet access service does not control sessions and does not have

⁶² H.R. Rep. at 22, 1994 U.S.C.C.A.N. at 3502.

access to session information. At best, BellSouth may be able to detect that a request for a session has occurred; however, BellSouth would have no idea whether or not the session request was successful. The entity that controls the session, in most cases the Internet service provider, is the only source that has definitive knowledge about the status of user sessions. Similarly, reliable information about IP addresses can only be obtained from the Internet service provider because it is the entity that performs IP address assignment; the broadband transport provider does not.

2. ***Information about changes to the subject's service or account profile, which could include, for example, new or changed logins and passwords.*** Information about changes to a subject's service or account profile does not constitute call-identifying information as defined by the statute. Because this information does not identify "the origin, direction, destination, or termination of each communication,"⁶³ a carrier is not required to provide it as call-identifying information under CALEA. This category of information is somewhat analogous to the "feature status" message functionality previously sought as call-identifying information by law enforcement and rejected by the Commission as unnecessary.⁶⁴ The "feature status" capability would have required carriers to notify law enforcement when specific subscription-based calling services were added to or deleted from the facilities under surveillance. Although the Commission concluded that these messages could be useful to law enforcement, it found that CALEA did not mandate the provision of this capability, because a "feature status" message does not constitute call-identifying information as defined by

⁶³ 47 U.S.C. § 1001(2).

⁶⁴ See *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, *Third Report and Order*, 14 FCC Rcd 16794, 16841-42, ¶ 111 (1999).

CALEA.⁶⁵ In light of the above, the Commission should find that information about changes to a subject's service or account profile is not call-identifying information required under CALEA. In addition, law enforcement is able to obtain such information today by issuing a subpoena to the Internet service provider.

3. Information about packets sent and received by the subject, including source and destination IP addresses, information related to the detection and control of packet transfer security such as those in VPN, as well as packet filtering to favor certain traffic going to or from certain customers. From the perspective of a provider of broadband transport, access to the information above would require full packet inspection or filtering of a customer's bitstream. BellSouth as a broadband transport provider does not have the technical capability to readily segregate an individual customer's data because individual customer traffic is aggregated in ATM circuits. Thus, regardless of whether or not this category of information is deemed to be "call-identifying information," it is not reasonably available.

The isolation of individual customer data would require a complete redesign of BellSouth's network. Today, as a transport provider, BellSouth's network (like most carrier networks) 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. Many new enhanced services require the establishment of multiple sessions and multiple IP addresses. Requiring broadband transport providers to isolate individual customer data could adversely affect an end user's ability to access these enhanced capabilities and services. Moreover, law enforcement surveillances would be jeopardized because the special switching of bitstreams in order to isolate

⁶⁵ See *id.*

individual customer data could make surveillances detectable by a target by creating observable latency.

Although Internet service providers will have access to some additional information beyond that reasonably available to the broadband transport provider, limitations in breaking open full packets exist for these entities as well. Similar to broadband transport providers, information is reasonably available to an Internet service provider only if it is within that provider's control and the provider uses the information to provide its CALEA-covered service to its customers.

In sum, the Commission need not clarify what constitutes "call-identifying information" in the context of broadband services. As indicated above, CALEA charges the industry with defining, through standards, how providers implement the CALEA assistance capability requirements, including applying the statute's definition of "call-identifying information" to broadband services. Only if an entity petitions the Commission claiming an absence or deficiency of standards should the Commission become involved in the process of prescribing rules regarding "call-identifying information."

VI. THE COMMISSION SHOULD NOT ADOPT LAW ENFORCEMENT'S PROPOSED FRAMEWORK FOR BENCHMARKS, COMPLIANCE DEADLINES, AND EXTENSIONS.

BellSouth fully supports the Commission's decision not to adopt law enforcement's proposed framework for CALEA benchmarks and compliance deadlines.⁶⁶ Notwithstanding this support, BellSouth finds the Commission's proposal for seeking relief from the Commission to lack the balance and flexibility sought by Congress. Although perhaps not the intended goal, the

⁶⁶ See Notice, ¶ 91.

effective result of the proposed framework for seeking relief from the Commission makes such relief nearly impossible. As discussed more fully below, this approach is inconsistent with CALEA.

Recognizing the immense responsibility placed on the industry to satisfy CALEA, Congress included several provisions designed “to ease the burden on industry.”⁶⁷ Included among these provisions is the right to seek one or more extensions from the Commission pursuant to Section 1006(c) (“Section 107 petitions”).⁶⁸ In addition, CALEA allows providers to petition the Commission to find that CALEA compliance for certain services or equipment is not “reasonably achievable.”⁶⁹ The Commission cannot – and should not – seek to eviscerate the balanced approach intended by Congress.

A. BellSouth Supports a Blanket Extension for Packet-Mode Communications.

BellSouth supports the Commission’s suggested blanket transition period to afford affected providers an adequate opportunity to become CALEA-compliant for packet-mode communications.⁷⁰ The Commission has granted similar industry-wide CALEA extensions in the past, and it is appropriate to do the same here.⁷¹ However, instead of the 15-month timeframe advocated by law enforcement, BellSouth supports a minimum 24-month transition period, which is consistent with the statutory two-year period for extensions in Section 1006(c)(1).

⁶⁷ H.R. Rep. at 18, 1994 U.S.C.C.A.N. at 3498.

⁶⁸ 47 U.S.C. § 1006(c)(2).

⁶⁹ *Id.* § 1008(b).

⁷⁰ *Notice*, ¶ 101.

⁷¹ *See id.*

Although a two-year timeframe probably will not 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, it is more reasonable than the arbitrary 15-month deadline advocated by law enforcement. Any transition period adopted by the Commission must take into account the fact that certain services and providers that are not “telecommunications carriers” could become subject to CALEA for the first time. In addition, these providers traditionally have not been actively involved in the CALEA standards-setting process or negotiations with vendors to develop and procure CALEA-complaint equipment. Therefore, it is unreasonable to expect such providers to achieve full compliance in a 15-month (or even two-year) period, especially if history is any indication of the future. Accordingly, any blanket transition period established by the Commission must take into account factors such as the length of time required to develop standards applicable to new services and new providers, as well as the time necessary to design, manufacture, test, and install CALEA-compliant equipment and software. At a minimum, the Commission should adopt a two-year transition period for packet-mode compliance. Moreover, this blanket extension should not adversely affect a provider’s statutory right to seek additional relief from the Commission pursuant to Section 1008(b), discussed more fully below.

B. The Commission Should Modify Its Proposed Framework for Considering Section 109(b) Petitions.

BellSouth also submits that the Commission should modify the proposed framework for considering “reasonable achievability” petitions (also known as Section 109(b) petitions). Under Section 1008(b), a carrier may petition the Commission to find that compliance with CALEA is not “reasonably achievable” for equipment, facilities, or services deployed after January 1,

1995.⁷² In making its determination, the Commission must consider eleven factors, one of which is “the effect on public safety and national security.”⁷³ The Commission proposes to assign substantial and greater weight to national security and public-safety related concerns than the other 10 factors, which include, among other things, (1) the effect on rates for basic residential telephone service; (2) the need to protect the privacy and security of communications not authorized to be intercepted; (3) the need to achieve the CALEA requirements by cost-effective methods; (4) the effect on the nature and cost of the equipment, facility, or service.

While BellSouth recognizes the heightened emphasis on national security following the events of September 11, 2001, BellSouth cautions the Commission against dismissing or minimizing the other statutory factors. Congress specifically included for Commission consideration criteria such as privacy, costs, and the effect on ratepayers of CALEA implementation, and the Commission is obligated to consider all of these factors. Congress did not intend public safety and national security to trump all of the other factors. If Congress had intended such a result, it would have listed the other criteria as discretionary items to consider. However, it did not. Indeed, the statute explicitly states that the Commission “shall consider the following factors.”⁷⁴ To ensure compliance with the statute, the Commission must not permit national security alone to be used as a basis for denying all Section 109(b) petitions. Law enforcement has not submitted any evidence in this proceeding to demonstrate that it has been unduly hampered in its national security investigations as a result of not having yet-to-be defined CALEA functionality for the surveillance of information services and other emerging services.

⁷² 47 U.S.C. § 1008(b).

⁷³ *Id.* § 1008(b)(1)(A).

⁷⁴ *Id.* § 1008(b)(1) (emphasis added).

Law enforcement remains able to obtain electronic surveillance information for electronic communications under existing wiretap laws.

In addition, the Commission should not dismiss automatically a Section 109(b) petition because it does not satisfy all of the detailed information requirements proposed in the *Notice*. The Commission tentatively concludes that it should require petitioners to submit detailed information about discussions and negotiations with switch manufacturers, other equipment manufacturers, and third party CALEA service providers to support Section 109(b) petitions. Also, carriers are expected to provide detailed cost data, including “copies of all offers, bids, and price lists negotiated with manufacturers and third party CALEA service providers.”⁷⁵

The absence of the information above should not result in an automatic dismissal of a Section 109(b) petition. Because the information requirements, if adopted, would be either new or more extensive than previous requirements, it would be unreasonable to hold providers to such a high evidentiary standard. Such information may not be available on a retrospective basis because providers have never been under any obligation to provide it to the extent sought by the Commission in the *Notice*. Also, the cost support and documentation sought by the Commission may not be available due to non-disclosure agreements. Manufacturers and vendors may not agree to permit the disclosure of cost information, even assuming confidential treatment of such information. In light of the above, providers should not be penalized by an automatic dismissal of a Section 109(b) petition if all of the information requirements are not met. The statute obligates the Commission to review these petitions and to base its conclusion on the factors identified in Section 1008(b).

⁷⁵ *Notice*, ¶ 105.

C. The Commission Should Not Establish Benchmarks and Interim Deadlines.

The Commission should not adopt law enforcement's proposals to establish CALEA benchmarks and compliance deadlines similar to those adopted for E911 implementation.⁷⁶ The Commission is correct when it states that "Law Enforcement's goal can be achieved without us imposing the implementation deadlines and benchmark filings it requests."⁷⁷ Notwithstanding this position, the Commission asks for more extensive comment on law enforcement's initial benchmark proposal.⁷⁸

The proposal advocated by law enforcement is not only inconsistent with the statute but also unnecessary and administratively burdensome. As an initial matter, Section 229(a) cannot be read so broadly as to vest the Commission and law enforcement with authority solely reserved for the courts – to determine whether a provider is in compliance with CALEA and to enforce compliance.⁷⁹ It strains credulity to think that Section 229 gives the Commission more enforcement authority than that which Congress expressly established for the courts. Section 229 is not a delegation of open-ended authority to the Commission. Further, as discussed more fully below, if law enforcement wants to challenge a carrier's compliance with CALEA, it may turn to the courts as Congress intended.

The Commission may not usurp authority specifically designated to the courts. CALEA mandates that any enforcement order issued by a court specify both a reasonable time and the conditions for compliance. Moreover, a court may not:

⁷⁶ *See id.*, ¶ 108.

⁷⁷ *Id.*, ¶ 91.

⁷⁸ *Id.*, ¶ 108.

⁷⁹ 47 U.S.C. § 1007.

- (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.⁸⁰

The government's benchmark and compliance proposal, however, would eliminate these various statutory limitations, which restrict a court's enforcement powers. Under law enforcement's plan, a carrier's inability to meet the proposed compliance benchmarks would constitute an automatic violation that would be referred to the Enforcement Bureau and potentially subject that carrier to penalties and sanctions.⁸¹ The statute affords carriers more flexibility than the government's proposal in that Section 1007 requires a court, in issuing an enforcement order, to consider the specific circumstances surrounding law enforcement's request, as well as the burdens and costs imposed upon the provider to achieve compliance. In making this determination, a court also is obligated to consider "the good faith efforts to comply in a timely manner, any effect on the carrier's, manufacturer's, or service provider's ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and such other matters as justice may require."⁸² Law enforcement's proposed framework of benchmarks and compliance deadlines, however, is completely void of the flexibility

⁸⁰ *Id.* § 1007(c).

⁸¹ *See* Joint Petition at 42-47.

⁸² 47 U.S.C. § 1007(b).

contemplated by Congress and seeks to vest the Commission with more authority than that given to the federal courts. As such, the benchmark proposal must fail.

Further, CALEA recognizes that a carrier's inability to meet the assistance capability requirements of Section 103 does not constitute a *per se* violation of the statute that subjects the provider to automatic enforcement. Section 1007 permits a court to issue an enforcement order under two express conditions:

- (1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and
- (2) compliance with the CALEA requirements is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken.⁸³

Under the first prong, a court should not issue an enforcement order if another carrier can provide law enforcement with the necessary intercept capabilities. The legislative history states as follows:

[T]he court must find that law enforcement has no alternatives reasonably available for implementing the order through the use of other technologies or by serving the order on another carrier or service provider. Essentially, the court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception.⁸⁴

Second, a court cannot issue an enforcement order unless compliance is “reasonably achievable” through the application of available technology, or would have been reasonably available if timely action had been taken. Congress has interpreted “reasonable achievability” to include an analysis of costs imposed on the provider to meet its CALEA obligations. The legislative history is clear on this point:

⁸³ *Id.* § 1007(a).

⁸⁴ H.R. Rep. at 28, 1994 U.S.C.C.A.N. at 3508.

Of necessity, a determination of ‘reasonably achievable’ will involve a consideration of economic factors. This limitation is intended to excuse a failure to comply with the assistance capability requirements or capacity notices where the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features. This subsection recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of this bill.⁸⁵

Law enforcement’s benchmark and compliance proposal as well as the Commission’s proposal to minimize cost as a factor in considering whether information is “reasonably available” are flawed because they both fail to incorporate the “reasonable achievability” standard and cost considerations that permeate the statute. Section 1006(c) authorizes the Commission to grant an extension request if it determines that compliance with the assistance capability requirements is not “reasonably achievable.”⁸⁶ In addition, under Section 1008(b), a carrier may petition the Commission to find that compliance with CALEA is not reasonably achievable for equipment, facilities, or services deployed after January 1, 1995.⁸⁷ In making its determination, the Commission must consider “whether compliance would impose significant difficulty or expense on the carrier or on the users of the carrier’s systems.”⁸⁸ Other factors to be considered include (1) the effect on public safety and national security; (2) the effect on rates for basic residential telephone services; and (3) the need to achieve the capability assistance requirements by cost-effective methods.⁸⁹ Indeed, as Congress explained, “[o]ne factor to be considered when determining whether compliance is reasonable is the cost to the carrier of

⁸⁵ H.R. Rep. at 28-29, 1994 U.S.C.C.A.N. at 3508-09.

⁸⁶ 47 U.S.C. § 1006(c)(2).

⁸⁷ *Id.* § 1008(b).

⁸⁸ *Id.*

⁸⁹ *Id.* (emphasis added).

compliance compared to the carrier's overall cost of developing or acquiring and deploying the feature or service in question.”⁹⁰

Thus, adopting compliance benchmarks and deadlines without regard to costs is impermissible under CALEA. Congress not only directs the courts to consider cost in determining whether compliance is “reasonably achievable,” but also instructs the Commission to consider reasonable achievability, costs, cost-effective methods, and the impact on ratepayers when promulgating CALEA requirements. In light of the foregoing, law enforcement's benchmark and compliance proposal must necessarily fail.

In addition to being inconsistent with the statute, establishing a framework of benchmarks is not only unnecessary but also administratively burdensome. As discussed more fully below in Section VII., if law enforcement wants to challenge a carrier's compliance with CALEA, it may turn to the courts. There is no need to subject the entire industry to benchmarks and interim deadlines.

Moreover, requiring carriers to submit multiple benchmark filings subject to Commission review and response would be administratively burdensome for the Commission. As the Commission recently concluded, “[w]e find it unreasonable to presume that Congress intended the Commission to inefficiently expend its resources by individually acting on potentially thousands of duplicative filings.”⁹¹ It is not practical to expect the Commission to review and respond to such a potentially large volume of interim filings. Further, as stated above and discussed more fully below, CALEA provides law enforcement with the ability to seek

⁹⁰ H.R. Rep. at 19, 1994 U.S.C.C.A.N. at 3499.

⁹¹ *Petition for the Extension of the Compliance Date under Section 107 of the Communications Assistance for Law Enforcement Act by AT&T Wireless Services, Inc., et al., Memorandum Opinion and Order*, 13 FCC Rcd 17990, 18010, ¶ 34 (1998).

enforcement through a federal court order. Accordingly, there is no need to adopt a framework of benchmarks and interim compliance deadlines.

VII. CALEA ENFORCEMENT LIES EXCLUSIVELY WITH THE FEDERAL COURTS.

The Commission's general enforcement authority under the Communications Act does not vest it with authority to enforce CALEA. The statute is clear – enforcement authority for compliance with the assistance capability requirements of CALEA lies exclusively with the federal courts, not the Commission. Section 1007 explicitly describes the courts' enforcement powers as follows:

A court shall issue an order enforcing this subchapter under section 2522 of Title 18, only if the court finds that—(1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and (2) compliance with the requirements of this subchapter is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken.⁹²

Had Congress intended the Commission to assume an enforcement role, it would have expressly provided for such responsibility. The statute states that only a court can “specify a reasonable time and conditions for complying with [an enforcement] order.”⁹³ While it is clear that CALEA grants the Commission certain responsibilities related to the implementation of CALEA, enforcement is not one of those duties. Therefore, law enforcement's request for enforcement action by the Commission must be denied as inconsistent with CALEA. Moreover,

⁹² 47 U.S.C. § 1007(a).

⁹³ *Id.* § 1007(b).

if law enforcement wants to challenge an entity's compliance with CALEA, it may do so in the federal courts, as was intended by Congress.

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

- (1) designate certain types of entities as "telecommunications carriers" subject to CALEA;⁹⁴
- (2) exclude certain classes or categories of telecommunications carriers from the definition of a "telecommunications carrier;"⁹⁵
- (3) in response to a petition, establish technical requirements or standards for complying with the assistance capability requirements of CALEA;⁹⁶
- (4) grant extension requests;⁹⁷
- (5) establish rules regarding systems security and integrity;⁹⁸
- (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;⁹⁹ and
- (7) in response to a petition, determine whether CALEA compliance is reasonably achievable.¹⁰⁰

Any actions taken by the Commission beyond those articulated above are outside of the scope of the Commission's authority. This includes the adoption of sections of CALEA as Commission rules as proposed in the *Notice*.¹⁰¹ Such an action would constitute circumvention

⁹⁴ *Id.* § 1001(8)(B)(ii).

⁹⁵ *Id.* § 1001(8)(C)(ii).

⁹⁶ *Id.* § 1006(b).

⁹⁷ *Id.* § 1006(c).

⁹⁸ *Id.* § 229.

⁹⁹ *Id.* § 229(e).

¹⁰⁰ *Id.* § 1008(b).

¹⁰¹ *See Notice*, ¶ 115.

of the statute's enforcement framework and would not withstand legal scrutiny. In a recent audit of the Department of Justice, even the auditor concluded that "CALEA does not give additional [enforcement] powers to the FCC."¹⁰² Clearly, the Commission may not exercise enforcement authority not granted to it by CALEA.

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. CALEA compliance is already challenging and costly without the added burden of disparate burdens of proof and enforcement mechanisms. Moreover, law enforcement has failed to demonstrate 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 that the government has ever sought 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.

VIII. ANY CALEA RULES ADOPTED BY THE COMMISSION MUST NOT STIFLE INNOVATION.

BellSouth supports the Commission's tentative decision to refuse to adopt law enforcement's proposals regarding the identification of future services and entities subject to

¹⁰² 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).

CALEA.¹⁰³ Law enforcement previously requested that the Commission establish presumptions that would make practically all future broadband services subject to CALEA and require carriers to file petitions for clarification with the Commission to determine whether current or planned equipment, facilities, or services are subject to CALEA.¹⁰⁴

As parties previously demonstrated and the Commission acknowledges, these proposals would impede significantly the advancement of broadband technology and chill innovation.¹⁰⁵ According to the Commission, the “statute and its legislative history seem to support . . . arguments that Congress did not intend that manufacturers or providers would be required to obtain advance clearance from the government before deploying a technology or service that is not subject to CALEA.”¹⁰⁶ In addition, Section 1002(b)(1) expressly precludes law enforcement from requiring or prohibiting any specific design of equipment, facilities, services, or features.¹⁰⁷ To avoid stifling technological advances in the communications industry and ensure that consumers are not deprived of new and improved broadband technologies, features, and services, the Commission should not require carriers to subject their current or future services and equipment development plans to prior Commission review through an administratively inefficient government pre-screening process.

¹⁰³ *See Notice*, ¶ 60.

¹⁰⁴ *See id.*

¹⁰⁵ *See id.*, ¶ 61.

¹⁰⁶ *Id.*

¹⁰⁷ 47 U.S.C. § 1002(b)(1).

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

The Commission should address the recovery of costs incurred by providers to implement CALEA. First, the Commission should modify its tentative conclusion “that carriers bear responsibility for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities.”¹⁰⁸ This tentative conclusion omits a critical limitation on a carrier’s financial responsibility. Specifically, if the Commission finds that CALEA compliance for equipment and facilities deployed after January 1, 1995 is not reasonably achievable, the government is responsible for paying the costs of compliance.¹⁰⁹ If the government refuses to pay for a carrier implementing the modifications and upgrades necessary to comply with CALEA, that carrier is found to be in compliance.¹¹⁰

Second, BellSouth supports an approach that would spread costs among the general public. The *Notice* repeatedly emphasizes the Commission’s desire to assist the law enforcement community in its efforts to fight crime and terrorism and protect the national security.¹¹¹ As the Commission recognizes, the Nation as a whole benefits from surveillance activities conducted using CALEA functionalities.¹¹² 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 programs. The source of this funding could be additional appropriations sought from Congress or a specific tax

¹⁰⁸ *Notice*, ¶ 125.

¹⁰⁹ 47 U.S.C. § 1008(b)(2).

¹¹⁰ *Id.* § 1008(b)(2)(B).

¹¹¹ *See Notice*, ¶¶ 16, 20.

¹¹² *See Notice*, ¶ 127.

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, the Commission should allow these providers flexibility in how they recover their CALEA implementation costs. Providers should have the discretion to absorb costs or pass them along to their 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.¹¹³

Regardless of whether the Commission permits providers to recover CALEA costs from their consumers, the government should not be excused from its financial obligations. Congress did not intend to saddle the communications industry or its consumers with all of the costs of building and maintaining the most effective and efficient surveillance system envisioned by law enforcement. Neither carriers nor consumers of communications services should be expected to absorb the full costs of CALEA implementation given the widespread national benefits of CALEA-supported services.

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

The trusted third party model may be an appropriate mechanism to enable providers to achieve CALEA compliance under certain conditions. As the Commission notes, this approach is being used by law enforcement today.¹¹⁴ BellSouth does not object to allowing law

¹¹³ 47 U.S.C. § 229(e).

¹¹⁴ *Notice*, ¶ 69.

enforcement to continue to contract with these third parties in order to obtain the information it seeks. Under this scenario, providers would deliver a duplicate packet stream (combined call content and call-identifying information) to the third party. The trusted third party would, in turn, analyze the data and separate call content from call-identifying information in order to provide law enforcement with only that information to which it is legally entitled.

Any trusted third party model should include the following safeguards. First, the use of a trusted third party should be voluntary, not mandatory. Providers must retain the flexibility to implement CALEA solutions within their own networks to satisfy their CALEA obligations if they so choose.

Second, the trusted third party should not be owned, governed, or controlled by law enforcement. Maintaining an independent entity without ties to the government avoids potential conflicts of interest or perceptions of impropriety.

Third, individual carriers should not be required to establish contracts directly with a trusted third party. A more efficient approach is for law enforcement to contract directly with the trusted third party, as is done today, and to instruct providers to send information to the entity as law enforcement's designated agent. This approach avoids thousands of carriers having to negotiate individual agreements with the trusted third party.

Fourth, the trusted third party model should not be used to shift the cost burden to the industry. As the Commission notes, this model is being used currently by law enforcement with the government compensating the trusted third party for services rendered. This approach is functioning today, and there is no demonstrated reason to disturb this model.

XI. CONCLUSION

As demonstrated above, many of the proposals set forth in the *Notice* go far beyond what is legally permissible under CALEA. The only way to achieve the objectives sought by the Commission and demanded by Law Enforcement is through a statutory amendment to CALEA. In the absence of such an amendment, the Commission is obligated to take a more balanced approach that satisfies Congress's objectives of preserving the ability of law enforcement to conduct lawfully authorized electronic surveillance, while simultaneously protecting the privacy of communications and not impeding the introduction of new technologies and services. In order to achieve this balance and ensure that any new rules fit within the scope of CALEA, the Commission should take the following actions:

1. Adhere to the law by concluding that broadband Internet access providers are information service providers that are exempt from the requirements of CALEA;
2. Establish an analytical framework that considers market conditions in order to determine whether a particular service meets the "substantial replacement" standard of CALEA and is therefore subject to the statute's assistance capability requirements;
3. Allow industry standards-setting bodies, in consultation with law enforcement, to complete efforts to establish appropriate standards governing packet-mode communications, including determining what information meets the statutory definition of call-identifying information for broadband transport, VoIP services, and emerging services;
4. 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;
5. Continue to decline to adopt law enforcement's proposed framework for CALEA benchmarks and deadlines;
6. Grant a blanket extension for packet-mode communications applicable to the entire industry upon adoption of a final order in this proceeding;

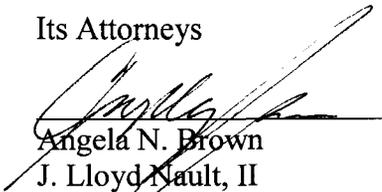
7. Recognize that CALEA enforcement lies exclusively with the federal courts and decline to establish a separate enforcement mechanism;
8. Continue to decline to adopt law enforcement's proposals regarding the identification of future services and entities subject to CALEA;
9. Find that the government 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 allow providers flexibility in recovering CALEA implementation costs; and
10. Allow for the voluntary use of trusted third parties as a means for providers to satisfy their CALEA obligations.

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

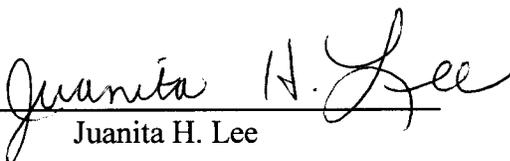
November 8, 2004

CERTIFICATE OF SERVICE

I do hereby certify that I have this 8th day of November 2004 served the following parties to this action with a copy of the foregoing **COMMENTS** by electronic filing to the parties listed below.

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
The Portals, 445 12 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



Juanita H. Lee