ORIGINA

RECEIVED

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

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

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

To: The Commission

COMMENTS OF AT&T CORP. REGARDING FURTHER NOTICE OF PROPOSED RULEMAKING ON CALEA CAPABILITIES

Mark C. Rosenblum
Stephen C. Garavito
Seth S. Gross
AT&T Corp.
Room 3252F3
295 North Maple Avenue
Basking Ridge, New Jersey 07920
(908) 221-4432

Douglas I. Brandon
Roseanna DeMaria
AT&T Wireless Services, Inc.
Fourth Floor
1150 Connecticut Avenue
Washington, D.C. 20036
(202) 223-9222

Dated: December 14, 1998

No. of Copies rec'd 0+6
List ABCDE

CONTENTS

SUMMARY i

I. CALEA CAPABILITIES 3

A. Defining Reasonably Available Call-Identifying Information 3

B. Punch List Capabilities 7

1. Content of Subject-Initiated Conference Calls 7

2. Party Hold, Join and Drop on Conference Calls 8

3. Subject-Initiated Dialing and Signaling 11

4. In-Band and Out-of-Band Signaling 12

5. Timing Information 14

6. Surveillance Status and Continuity Check 15

7. Feature Status 17

8. Dialed Digit Extraction 18

II. DISPOSITION OF JSTD-025 AND OTHER TECHNOLOGIES AND SYSTEMS 22

A. Remand for Amendment of JSTD-025 22

B. Commission's Role in Future Standards 23

C. Packet-Mode Communications 25

III. SECTION 107(b) FACTORS 26

A. The Unknown Cost of the Punch List 26

B. The Cost of JSTD-025 27

IV. CONCLUSION 30

SUMMARY

On November 5, 1998, the Commission released a Further Notice of Proposed Rulemaking (the "FNPRM") in which it tentatively concluded that, despite uniform industry opposition, certain additional surveillance capabilities should be added to the industry standard. AT&T continues to believe that the Communications Assistance for Law Enforcement Act ("CALEA") does not require, and in some cases prohibits, these enhanced surveillance features. For example, extraction and delivery of post-cut-through dialing or signaling on a pen register order violate both CALEA's requirement to protect the privacy of communications not authorized to be intercepted and the organic wiretap law itself.

Even if the punch list items yield call-identifying information as the Commission tentatively concludes, that information is not "reasonably available." For example, no system today generates party join and drop messages to dynamically report when parties enter or leave a conference call. The standard is not whether systems could be designed to make such information available, but rather, whether such information is reasonably available to a carrier at all.

AT&T supports remand of any changes in the standard to the industry standards setting body. However, the final order and standard will not be a checklist for compliance for other technologies for which industry members have yet to promulgate standards. Further, under CALEA, the Commission may not on its own take up a standards effort for other technologies. As to standards for packet-mode communications, the Commission should forbear, permitting industry to begin standards efforts on its own.

Finally, JSTD-025 carries a significant cost, and the additional DOJ advanced surveillance features will materially add to it. However, cost information is not now available. In the event that cost information becomes available, comment on the information will be required.

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

In the Matter of	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

To: The Commission

COMMENTS OF AT&T CORP. REGARDING FURTHER NOTICE OF PROPOSED RULEMAKING ON CALEA CAPABILITIES

On April 20, 1998, the Federal Communications Commission ("Commission") released a Public Notice requesting comment on the scope of the assistance capability requirements of the Communications Assistance for Law Enforcement Act ("CALEA") in response to various petitions filed under Section 107 of CALEA.[1] AT&T Corp., for itself and AT&T Wireless Services, Inc. ("AWS") (collectively "AT&T"), pursuant to Section 1.405 of the Commission's Rules, 47 C.F.R. §1.405, submitted both comments and reply comments supporting a narrow reading of CALEA's requirements as intended by Congress.[2]

---

1 *In the Matter of Communications Assistance for Law Enforcement Act,* Public Notice, DA 98-762, CC Docket No. 97-213 at 4 (released April 20, 1998) (the "Public Notice"). The petitions included: The Center for Democracy and Technology ("CDT") Petition for Rulemaking under Sections 107 and 109, filed March 26, 1998 ("CDT Petition"); Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI")(collectively, "DOJ") Joint Petition for Expedited Rulemaking, filed March 27, 1998 ("DOJ Petition"); Cellular Telecommunications Industry Association ("CTIA"), Petition for Rulemaking, filed July 16, 1997 ("CTIA Petition"); and Telecommunications Industry Association ("TIA"), Petition for Rulemaking, filed April 2, 1998 ("TIA Petition").

2 Comments of AT&T Corp. Regarding Scope of CALEA Capabilities [hereinafter "AT&T Comments"], CC Docket No. 97-103, at 1 (May 20, 1998) and Reply Comments of AT&T Corp. Regarding Scope of CALEA Capabilities [hereinafter "AT&T Reply Comments"], CC Docket No. 97-103, at 1-2 (June 12, 1998).

On November 5, 1998, the Commission released a Further Notice of Proposed Rulemaking (the "FNPRM") in which it tentatively concluded that, despite uniform industry opposition, certain additional surveillance capabilities should be added to the industry standard through industry amendment of that document.[3] The Commission sought further comment on a variety of issues, including its tentative conclusions about which capabilities are or are not required by CALEA, how the Commission should consider the factors under Section 107(b) in its decision, and the manner in which the industry standard should be amended to meet the Commission's final order when issued. AT&T submits these further comments in response to the FNPRM.

As a general comment at the outset, AT&T commends the Commission on the apparent thoughtfulness and thoroughness of its FNPRM. While AT&T does not agree with all of the Commission's tentative conclusions for reasons set forth below, AT&T nonetheless appreciates the careful analysis conducted by the Commission. Further, AT&T especially supports the Commission's determination that its final order will be implemented through amendment of the industry standard under TIA auspices. Whatever the outcome of these proceedings, industry engineers working in consultation with law enforcement will be best situated to effect the necessary changes to JSTD-025 in an expeditious manner.

These Comments will first explain AT&T's concern with the tentative conclusions reached by the Commission in the FNPRM regarding DOJ's so-called "punch list" capabilities. AT&T continues to believe that CALEA does not require these advanced surveillance features. AT&T also continues to believe that the Commission should set forth clear principles for determining when call-identifying information is "reasonably available."[4]

---

3 *In the Matter of Communications Assistance for Law Enforcement Act,* CC Docket No. 97-213, Further Notice of Proposed Rulemaking (released Nov. 5, 1998).

4 *See* AT&T Comments at 7 n.22.

Next, AT&T discusses the Section 107(b) factors. AT&T, like all carriers with obligations under CALEA, is concerned about the cost impact of CALEA on subscribers. In particular, AT&T is concerned that JSTD-025 carries a significant cost, and the additional DOJ-advanced surveillance features will materially add to it. AT&T also is concerned about the direct impact of CALEA and the punch list additions on competition and innovation. The Commission has the power to reject any capability that fails to meet Section 107 factors.

Although an adequate and accurate cost record must exist before the Commission can act, such cost information has not yet been placed in the record. It is clear that further comment will be necessary unless manufacturers and the FBI submit such cost information, openly and available for comment by all, in this proceeding.

AT&T also continues to support remand of any changes in the standard to the industry standards setting body. However, the Commission should not look on its final order as a checklist for compliance for other technologies where industry members have yet to promulgate a standard; nor should the Commission on its own take up a standards effort for these emerging communications enterprises. Finally, AT&T comments on the need for further proceedings on packet-mode communications.

I. CALEA CAPABILITIES

A. Defining Reasonably Available Call-Identifying Information

Under CALEA, not all call-identifying information need be provided to law enforcement; carriers only have the obligation to provide *reasonably available* call-identifying information. Yet, as the Commission notes, CALEA does not define the term "reasonably available."[5]

---

[5] FNPRM at ¶ 25-26.

However, in crafting JSTD-025, industry considered the terminology from a technical perspective and defined it as follows:

> Call-identifying information is reasonably available if the information is present at an Intercept Access Point (IAP) for call processing purposes. Network protocols (except LAESP) do not need to be modified solely for the purpose of passing call-identifying information. The specific elements of call-identifying information that are reasonably available at an IAP may vary between different technologies and may change as technology evolves.[6]

AT&T supports the definition adopted by industry in JSTD-025.

As a matter of statutory interpretation, the term "reasonably available" must be construed narrowly as a limitation on the requirement to provide call-identifying information in the first instance.[7] Congress specifically mandated a narrow interpretation of CALEA's requirements in order to prevent industry from being required to make design changes in systems to create new forms of call-identifying information or to make previously unavailable call-identifying information *available in all cases* in the future. Indeed, this important limitation on the call-identifying information to which a carrier must ensure government access informs the very meaning of what constitutes call-identifying information. That is why the industry overwhelmingly supported defining call-identifying information as the dialing or signaling information used in call setup.[8]

---

6 JSTD-025 at § 4.2.1.

7 Congress directed that the Commission interpret the requirements of CALEA narrowly. *See* H.R. Rep. No. 103-827, 103d Cong., 2d Sess., at 23 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3502-03 [hereinafter "House Report"] ("The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements."). *See also* 2A Norman J. Singer, Sutherland *Statutory Construction* § 47.11 (5th Ed. 1993) (clauses that limit the generality of a rule are narrowly construed).

8 *See* AT&T Comments at 6-7. The Commission has stated that it "propose[s] to interpret these provisions narrowly. . . . [and to] look to the plain language, its context, and, if necessary, any legislative history that assists in ascertaining Congressional intent." FNPRM at ¶ 25. However, the Commission fails to define call-identifying information or its component parts (*i.e.*, origin,

(footnote continued on next page)

CALEA defines call-identifying information as follows:

> 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 equipment, facility, or service of a telecommunications carrier.[9]

JSTD-025 uses the precise statutory definition.[10] It further defines the terms "origin, direction, destination, or termination" as follows:

> **destination** is the number of the party to which a call is being made (e.g., called party); **direction** is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); **origin** is the number of the party initiating a call (e.g., calling party); and **termination** is the number of the party ultimately receiving a call (e.g., answering party).[11]

These definitions are consistent with CALEA's legislative history. For voice communications, Congress states that "call-identifying information" is "the numbers dialed or otherwise transmitted for the purpose of routing calls through the carrier's network."[12] For pen register cases, Congress understood call-identifying information to be limited to "the

---

(footnote continued from previous page)

direction, destination, termination). Rather, the Commission tentatively concludes in contradictory fashion, for example, that location information identifies "the 'origin' or 'destination' of a communication," FNPRM at ¶ 52, and that location should be construed to mean "the beginning and termination of a call." ¶ 55. The lack of precision inherent in this definition comes from a failure to define the individual terms as industry has done in JSTD-025.

9 47 U.S.C. § 1001(2).

10 JSTD-025, Section 3.0, Definitions. As a further rule of statutory construction, the Commission should have given deference to the technical meaning of call-identifying information proposed by industry. *See* 2A Sutherland *Statutory Construction* § 47.29 (citing *Corning Glass Works v. Brennan,* 417 U.S. 188 (1974) ("working conditions construed to have technical meaning in industrial usage")).

11 JSTD-025, Section 3.0, Definitions.

12 House Report at 3501.

numbers dialed from the facility that is the subject of the court order."[13] And for trap and trace investigations, Congress limited call-identifying information to "the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order."[14]

The Commission should not have strayed in the FNPRM from this analytically sound approach to call-identifying information. However, if the Commission stands by its tentative conclusions, JSTD-025's reasonably available definition will need to be amended. In that event, the Commission should provide some additional guideposts.

For example, the Commission should acknowledge as a general principle that processing that takes place entirely within the terminal or other subscriber-owned or maintained equipment is not reasonably available even if it is call-identifying, because the network is not aware of it. While not intended to serve this exact point, the Commission uses a similar example involving customer premises equipment ("CPE") in the FNPRM that actually illustrates this principle.[15] Thus, whatever the end user device that performs the processing, so long as no network signal is generated, the information is not reasonably available.

AT&T urges the Commission to also reject the notion that any signaling that can be perceived by the subscriber is reasonably available call-identifying information whether or not the facilities under surveillance generate the signal or act on it. While this point is addressed in more detail below in the in-band signaling section, the general principle should be adopted by the Commission. Many of these signals are generated solely because of human

---

13 *Id.*

14 *Id.*

15 *See, e.g.,* FNPRM at ¶ 92 ("to the extent that CPE is used to perform any of the functions described here [i.e., subject-initiated dialing], and no network signal is generated, that information will not be reasonably available to a carrier, and thus, should not be required to be provided.")

expectations (e.g., hearing a busy signal if the call cannot be connected) and market adoption of new technologies. In other words, the signals, while generated by some network, serve no call processing purpose other than to mimic known telephony sounds.

With these principles in mind, AT&T addresses the specific punch list items below.

B. Punch List Capabilities

1. Content of Subject-Initiated Conference Calls

In concluding that provision of the content of subject-initiated conference calls is a CALEA-mandated technical requirement, the Commission did not address the extra provisioning of channels necessary to monitor both the subscriber's new call and the conference call on hold.[16] The first thing the Commission must do is make clear that this capability is conditional and subject to adequate provisioning to monitor all active surveillance.[17]

Further, on conference call monitoring in particular, CALEA applies to communications carried by the carrier within a service area to or from the equipment, facilities, or services *of a subscriber.*[18] While conference calling as described in the FNPRM is a "service" to which a customer can subscribe as part of his or her suite of services, not all conference call services are subscriber-based. One-time, on-demand services like "Meet Me" conference calling where the carrier or a third party provider makes a conference bridge available to any comer, whether or not they are a subscriber to any specific carrier, are not

---

16 *See* AT&T Comments at 4-5.

17 Under JSTD-025, channels are provisioned on a first come, first served basis. If a law enforcement agency provisions three lines for three surveillances and a fourth line is needed because one of the targets has conference calling services, the carrier should not be in violation of the standard because it cannot service the wiretap.

18 47 U.S.C. § 1002(a)(1).

covered by CALEA. There is no subscriber and therefore no subscriber equipment, facilities or services to be invoked. These types of services should be not be included in any final order addressing conference calling.[19]

2. Party Hold, Join and Drop on Conference Calls

The Commission tentatively has concluded "that party hold/join/drop information falls within CALEA's definition of 'call-identifying information' because it is 'signaling information that identifies the origin, direction, destination, or termination of each communication generated or received' by the subject."[20] There are several serious flaws in the Commission's reasoning.

First, the party join and drop messages[21] cannot be "signaling information" that identifies anything for the simple reason that carriers generate no such signals today to be reported. DOJ admits that they do not receive such information today.[22] Even if such information were call-identifying, which it is not for the reasons indicated below, by no stretch of the imagination or plain statutory construction could these messages be said to report *reasonably available* call-identifying information. The information is not available today at all. To require that carriers design such information into future equipment would be to make

---

19 AT&T also notes that applying the call-identifying information requirements of JSTD-025 to "Meet Me" conference calling would be very difficult, complex and costly. The conference bridge itself would be a separate Intercept Access Point ("IAP") in essence and would require a content channel to be dedicated for every participant. There is no way of knowing whether the target is participating or which participant has placed the conference call on hold. Under the DOJ interpretation, the subject need not even participate in the bridged call for the monitoring to take place. *See* Declaration of Kirk Carlson at 9, attached to Comments of CTIA as Exhibit 1 (May 20, 1998).

20 FNPRM at ¶ 85.

21 The party hold message can be dealt with better as subject-initiated signaling.

22 DOJ Petition at 42 ("law enforcement was unable to obtain information that a particular participant was placed on hold during, or dropped from, a multi-party call.")

the "reasonably available" limitation on providing call-identifying information "mere surplusage."[23] All call-identifying information perforce will be *always available* in the future under such reasoning. Thus, the Commission rewrites CALEA when it turns a reasonably available standard into an inquiry about what could be made *always available* in the future.[24]

Second, carriers today do not dynamically report any party's addition to or drop from a conference call let alone the actions of a serendipitous subject of surveillance. This is the case because there is no business purpose for doing so -- the relevant information for billing is that the subject uses specific facilities for the duration of the call. Whether a party joins or drops from a call has no bearing on the continuity of a call or the communications that may be made during the call.[25]

Third, the Commission's logic that such signals, if they existed, would report the origin, destination, direction or termination of a *communication* reveals a deeper flaw in the logic. *Communications* are not one-way legs of a call. There is no current understanding in the law or in engineering parlance that a call leg constitutes a call or communication.[26] Yet, the Commission suggests that party messages are required to permit call-identifying information to be associated with the content of the communication to which it pertains.[27]

---

23 As the Commission notes, rendering a provision in a statute mere surplusage conflicts with the rules of statutory construction. FNPRM at ¶ 58 n. 106 (citations omitted).

24 FNPRM, at ¶ 86 (noting that such signals "could not be reasonably made available" when provided by customer premises equipment because no network signal is generated).

25 There can be no doubt that the relevant information is provided to law enforcement under JSTD-025. Law enforcement is notified by an origination message when the subject initiates a call. They receive a second origination message when the subject places the associate on hold and dials another party. They receive a change message when the parties are joined together in a three-way call. And, they receive a close message when the call is ended, whether or not one of the associates hangs up before the subject or other associate and even if one of the associates simply has left the phone off-hook and walked away. CALEA requires no more.

26 *See* 18 U.S.C. § 2510(1), (2) & (12) for definitions of "communications."

27 Of course, JSTD-025 ensures that all of the call content is delivered to law enforcement.

Having defined communication in an arbitrary manner as a call leg, the Commission would require carriers to create a hitherto nonexistent signal to bootstrap its requirements.

Fourth, the Commission notes that without these messages it would be unable to determine who is talking to whom or to focus on the subject's role in the conversation.[28] As AT&T noted in prior comments, and as the Commission acknowledged in the FNPRM, these messages will not tell law enforcement whether a party hears or doesn't hear any communication.[29] They do nothing more than testify to the existence of a connection between parties. While they may eliminate one party from a conversation at the relevant investigative point, they do not affirmatively testify that a party heard or participated in the criminal conversation.[30]

Finally, should the Commission sustain its tentative conclusion, it should do no more than require that industry, on amendment of JSTD-025, provide for dynamic reporting of participant changes in a subscriber-initiated conference call. The industry may have more efficient or effective ways than party messages to report joins and drops from conference calls. Industry should be afforded in the first instance the opportunity to optimize the existing standard for reporting additional requirements imposed by the Commission. The standards process is ideally suited to vet such alternatives.

---

28 FNPRM at ¶ 85. The Commission apparently would read CALEA to require a carrier to report who said what to whom and to do so with a message. This is more than an arbitrary reading of CALEA, it is a significant expansion of existing wiretap capabilities.

29 AT&T Comments at 10-11; FNPRM at ¶ 81.

30 Even if the Commission requires that carriers generate such signals in the future to report dynamically participant changes in a conference call, applying the Section 107(b) cost-benefit analysis certainly justifies exclusion of this capability.

3. Subject-Initiated Dialing and Signaling

The Commission inappropriately has mixed several punch list requirements under the rubric of subject-initiated dialing or signaling. DOJ's goal with this punch list item is to obtain any signal generated by the subscriber that controls a call.[31] Industry has countered that signals such as a switchhook flash, hold key, flash key, transfer key, or conference key do not identify the origin, destination, direction or termination of a call and that other messages in the standard are designed to capture the relevant call-identifying information.[32]

Notwithstanding, the Commission tentatively has concluded that such signaling is call-identifying, but does so apparently by relating the signals to specific features. That is, the Commission's references to call-forwarding signaling and call-waiting signaling implies network signals to terminal lamps rather than call control signals.[33] It then discusses remote activation of services from other than the subscriber's equipment, which more appropriately is discussed as feature status reporting. The only rationale for its tentative conclusion that appears to be on point to this punch list item is the claim that such signals are needed to

---

31 DOJ Reply Comments at 46-50.

32 *See, e.g.,* TIA Comments at 47-51. For example, a subscriber may place a call on hold using a flash key, which does in fact generate a signal, that under JSTD-025 is not reported. But when the subscriber initiates the second call to another party, under the industry standard, an origination message would be generated. If the subscriber using a conference key then combines the two calls into a single, three-way call, a signal is generated but not reported under JSTD-025 for the key stroke. But, under the industry standard, a change message would be generated. These are the messages that identify the call, not the invocation of the feature. The Commission also indicated without any specific analysis that signaling data showing that the subject is accessing voice mail is properly classified as call-identifying. FNPRM at ¶ 93. But to what "signal" does the Commission refer? Such access will always be driven by an origination message showing the dialing by the subject or it will be post-cut-through dialing or signaling that the accessing system does not detect. AT&T believes this "observation" by the Commission is erroneous.

33 FNPRM at ¶ 91.

permit association of the event with the content of the communication.[34] Thus, it is difficult for AT&T to comment on the tentative conclusion without understanding the Commission's rationale.

AT&T assumes that the Commission actually means that subject-initiated dialing or signaling that controls a call is call-identifying. Such signals include when a subject goes off-hook and then on-hook without dialing any digits, a switchhook flash, hold key, flash key, transfer key, or conference key. As noted above, AT&T disagrees with this conclusion.

Should the Commission proceed on the basis of its tentative conclusion, the general principle should be limited by the caveat that such signals must be reported only to the extent known to the accessing switching system. This important limitation also resolves any question regarding what is reasonably available to the carrier.[35]

4. In-Band and Out-of-Band Signaling

The Commission appears to have concluded, without any analysis, only that voice message waiting indicators are call-identifying.[36] As for other signals, the Commission then states that it will not decide whether they are call content or call-identifying; rather, the Commission requests comments only on what types of in-band and out-of-band signals are

---

34 FNPRM at ¶ 92. Here again the Commission defines a signal as call-identifying and then bootstraps its argument by saying that CALEA requires the signal to associate the event with the content of the communication. It is true that if information is call-identifying, it must be associated with the content of the communication to which it pertains, but that is not to say that all signals must be associated with a particular communication and therefore are call-identifying.

35 *See, e.g.,* FNPRM at ¶ 92 (CPE signals are not reasonably available).

36 FNPRM at ¶ 99.

"technical requirements."[37] The Commission cannot so easily sidestep its obligation under CALEA.[38]

AT&T submits that the Commission's difficulty here is the result of its failure to narrowly define, as Congress directed, call-identifying information to be "the numbers dialed or otherwise transmitted for the purpose of routing calls through the carrier's network."[39] Network signals such as busy tone, re-order tone or alerting tones do not route calls through a network and these most certainly were not the signals of interest to Congress in CALEA (or for that matter, law enforcement).

Once on the slippery slope of an open-ended definition of call-identifying information, it is easy to reach DOJ's bottom where carriers must provide *any* signaling that "can be sensed by the subject."[40] As AT&T noted in its previous comment, in that quagmire, DOJ abandons all pretense of such a signal identifying the origin, direction, destination or termination of a call; it simply seeks to know what the subject knows when he or she knows it.[41]

The Commission, if it insists on pursuing this punch list item, must identify general principles that can be applied to the multitude of network signals that currently exist and no doubt will be created in the future, whether in-band or out-of-band. One such principle must

---

37 FNPRM at ¶ 99. The Commission's statement here is in direct contrast to its determination that delivering the entire packet stream to law enforcement on a pen register order for call-identifying information would be the unauthorized delivery of call content. FNPRM at ¶ 63.

38 The Commission has an obligation under Section 107(b) to protect the privacy of communications not otherwise authorized to be intercepted. 47 U.S.C. § 1006(b).

39 House Report at 3501.

40 DOJ Petition at 47.

41 AT&T Comments at 11-12.

be that any such signals to be reported must be generated by the accessing system to which the surveillance order applies.[42]

Tones generated by other than the subject's switch are not reasonably available to the carrier but may be reasonably available to law enforcement through the content channel. Carriers should not have to design systems to extract another carrier's signaling and deliver it to law enforcement, especially when such signals have nothing to do with call routing but are the engineering equivalent of a placebo -- it makes the user of the service feel good to know that the line was busy, but it is not what ends the connection. In any event, under the industry standard, law enforcement is notified that a call was not completed because the facilities are released or closed.

AT&T would classify this punch list item as seeking "informational messages" rather than call-identifying information. The Commission simply should reject any such requirement as part of CALEA.

5. Timing Information

While AT&T can understand and even support a requirement for timing requirements in the standard, it must strongly disagree with the Commission's tentative conclusion that such requirements are "call-identifying information" or even that time stamps are the only correlation tool available to carriers.[43] While AT&T believes that timing should be left to

---

42 The DOJ Reply Comments seem to acknowledge this limitation clearly. DOJ Reply Comments at 57 ("The government's proposed rule is limited to in-band and out-of-band signaling 'from the subscriber's service' -- that is, signaling generated by the carrier providing the subscriber's service, not signaling generated by another carrier."). Yet, in post-filing contributions to the Enhanced Surveillance Standard ("ESS") committee, the FBI has stated once again that if the signal is "known" to the accessing system and perceptible by the subject, then it requires such signals to be delivered to law enforcement. This is why AT&T continues to urge the Commission to be scrupulous in its decision-making, clear in its principles, and narrow in its application of the CALEA requirements.

43 If timing requirements are "call-identifying," is the Commission willing to concede that in some implementations timing information will not be reasonably available?

individual implementations, especially inasmuch as CALEA is silent on the issue,[44] it can support reasonable timing requirements as good engineering practice in a standard.

Any such requirements should be message-specific, taking into account the nature of the event that prompts the message and its relative importance to law enforcement to know it, and would recognize that 100% guarantees do not apply in traditional telephony services. For example, the Commission should ensure that timing requirements apply to the first bit of a timing message measured at the point of demarcation between the carrier network and law enforcement's collection facilities. Further, the timing requirement for delivery should be expressed as a percentage so that delivery occurs within the timing requirement at least 95% of the time. This variable takes into account normal system operations and preserves the safe harbor for a carrier in the event a message arrives a second later than planned. The timing requirement must also recognize that there is no priority queuing for these messages and that congestion or flow control may occur that will delay delivery.

6. Surveillance Status and Continuity Check

AT&T agrees with the Commission's conclusion that a surveillance status message is not required by CALEA. When CALEA mandates that carriers "ensure" that they are capable of meeting Section 103's requirements, it does not impose a strict liability standard for technological failures in the system.[45] Rather, the "ensure" language imposes an obligation on carriers and manufacturers to design future equipment, facilities and services to support wiretaps.

---

44 *See* AT&T Comments at 14.

45 No doubt, during the course of any surveillance, a carrier's normal operational requirements may lead to service interruption generally and in some few cases (completely undocumented by law enforcement other than through anecdotes) surveillance may be interrupted by accident. System failures generally result in fault reports today.

Most recently, AT&T viewed the FBI punch list presentation that purports to represent its needs. The first example presented was intended to show law enforcement's need for a surveillance status message. The FBI presenters stated repeatedly that without this message, law enforcement would neither know that the surveillance had been provisioned nor be able to prove in court that earlier calls had not been received by the target. This, of course, is not quite right.

AT&T provisions thousands of electronic surveillances each year. AT&T either receives an order for surveillance and invariably calls the requesting agency to set up the surveillance, or more typically receives a call in advance of an order to begin the process of setting up the tap so information may be delivered immediately upon receipt of the order. Routinely, the law enforcement agency knows almost to the minute when the tap is installed and available to deliver information.

As to the notion that the surveillance evidence could be undermined in court, a carrier's call detail records will show what calls were made or received before, during and after the wiretap was provisioned. In short, the presentation of the surveillance status message was misleading. If the Commission viewed this presentation, it should carefully review the need for the message in the final order.

In any event, CALEA cannot be read to "freeze" carrier routine maintenance or operational activities such as system upgrades during wiretap activities for fear of interrupting the surveillance. Nor can (or did) Congress legislate away human error. Carriers and law enforcement must and do cooperate in surveillance activities. At any time law enforcement is concerned about the status of the surveillance, they simply can call the carrier as they do today. If a carrier discovers a problem today, it invariably fixes it and calls the agency to report it. CALEA should not be interpreted as a statute that allows the rare exception to

drive the requirement. Nor should the cost of providing convenient and automated features to law enforcement be foisted upon the industry and its subscribers.[46]

7. Feature Status

AT&T supports the Commission's conclusion that a feature status message is not required by CALEA.[47] Law enforcement itself admits that such information today is provided by manual means, i.e., a subpoena to the carrier. As the Commission notes, nothing in CALEA requires the automation of such a process[48] and, in fact, the complexity and cost involved to make such a procedure a matter of automated messaging likely would be enormous.

The one example raised by the Commission -- a change in the phone number of the facilities under surveillance -- is not a feature status message issue at all.[49] When a subscriber obtains a new line or changes phone numbers, he does not simply change the feature of an existing service, he obtains entirely new services. Law enforcement uses a continuing subpoena or order to require carriers to advise them of such changes *so they can obtain a new order for the surveillance.* The Commission should not imply that the same order can serve this change in facilities for surveillance purposes.

Just as with the surveillance status message, carriers and law enforcement must cooperate to identify changing circumstances in the surveillance. The process cannot possibly

---

46 The same rationale pertains to DOJ's request that C-tone be injected on a content channel as a means of determining whether the facilities under surveillance have an active call in progress. The current message set in JSTD-025 identifies when a call begins and ends and when connections are established. Nothing further is required. The Commission should be wary of any requirement that could be read to impose an anachronistic feature on future technologies just so law enforcement can hear what they were used to hearing in the analog world.

47 FNPRM at ¶ 121.

48 FNPRM at ¶ 119.

49 FNPRM at ¶ 122.

be automated because the variables are too great and would lead to over-engineering for what in reality is the exception case. The answer is that law enforcement must do what they do today -- and which CALEA did not contemplate altering -- request information by subpoena or order from a carrier to determine if the target has obtained a new phone number or second line.

8. Dialed Digit Extraction

In the face of the clear CALEA mandate that law enforcement use technology reasonably available to it to restrict the recording or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing,[50] it is ironic that the Commission would appear to require the accessing carrier to actually make technology available to receive rather than restrict such post-cut-through dialed digits.[51] The carrier with the surveillance order simply does not know which post-cut-through digits are dialing or signaling and which digits are other tones used to signal CPE or simply to play "Mary Had a Little Lamb" on the keypad. As Congress expressly stated, "dialing tones that may be

---

50 CALEA, Section 207 (codified at 18 U.S.C. § 3121(c)). Here again, Congress made clear that call-identifying information was limited to the numbers dialed for call processing.

51 It is all the more ironic given that FBI Director Freeh expressly testified before Congress that he did not want such post-cut-through dialing information:

> I do not want that access, and I am willing to concede that. What I want with respect to pen registers is the dialing information: telephone numbers which are being called, which I have now under pen register authority. As to the banking accounts and what movies somebody is ordering at Blockbuster, I do not want it, do not need it, and I am willing to have technological blocks with respect to that information.

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 103d Cong., 2d Sess., 50 (1994) (Testimony of FBI Director Freeh).

generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information."[52]

Yet, apparently because some post-cut-through dialed digits may connect to another carrier who then routes a call to its final destination, the Commission determines that such numbers must be call-identifying. No doubt, but not as to "communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service."[53] They are call-identifying as to the subscriber's other carrier and the subscriber's other services with that carrier and that other carrier's equipment and facilities that carry the communication, but not as to the carrier that has the current surveillance order. Thus, the Commission's conclusion that the accessing carrier has the obligation to acquire and deliver *any and all* call-identifying information no matter which carrier generates the information exceeds CALEA's limited mandate and should not be adopted.

The Commission correctly recognizes that post-cut-through digits are provided on the content portion of a connection.[54] For a carrier to extract such digits to provide to law enforcement, it must do so by accessing the content channel. On a pen register order, which most typically would be utilized to obtain such information because law enforcement otherwise would have a content channel, the carrier would have to intercept call content. By what authority does DOJ propose that a carrier, after CALEA, intercept call content on a mere pen register order? Indeed, carriers that provide post-cut-through information may face

---

52 House Report at 3501.

53 47 U.S.C. § 1002(a)(1) (emphasis added).

54 FNPRM at ¶ 128.

claims that they fail to protect the privacy of communications not authorized to be intercepted.[55]

The Commission also asks technologically how dialed digits can be extracted. DTMF tone extractors and decoders would be required for every surveillance target and every line potentially usable by that target with advanced calling features. In short, this is both a cost issue (the price of DTMF decoders) and a capacity issue. And the FBI seeks to impose the costs of both on carriers.

This is a capacity issue because carriers must have the capability to match with DTMF decoders the number of simultaneous wiretaps the government contends it may have to invoke pursuant to its final capacity notice.[56] With hundreds of thousands of lines that may need to be tapped *simultaneously* under the FBI's capacity notice, and the typical decoder costing over $200, the economic consequences of this tentative decision are enormous.

The costs are more out of line for AWS. One of its equipment vendors has advised that this may be the most difficult and costly of the punch list items to develop for the simple reason that wireless carriers do not use DTMF tone decoders in call processing.[57] Rather, in wireless communications, numbers dialed are sent over the air interface after the subscriber hits the <SEND> key. AWS has been told that major software changes will be required for its switches, including significant changes in the engineering and capacity guidelines for the mobile switching centers to accommodate the additional hardware required for each

---

55 47 U.S.C. § 1002(b)(3).

56 *See Implementation of the Communications Assistance for Law Enforcement Act,* Final Notice of Capacity, 63 Fed. Reg. 12,218 (Mar. 12, 1998).

57 In wireline systems, tone decoders circuits are used to gather digits as they are pulsed from a landline phone.

surveillance. In sum, for wireless, this is forcing a design on a carrier despite Congress's express prohibition of any such approach.[58]

Having extracted the tones with a DTMF recorder, does the Commission then propose that the carrier make the judgment as to which digits are call-identifying, which ones signal CPE and may not be provided, or which ones are inadvertent key pad strikes? Or does the Commission propose that the carrier provide all of the signals and leave it to law enforcement to "minimize" as they often say? The Commission should take note that there are no provisions in the pen register statute that require minimization; that requirement pertains only to content on a wiretap order.[59] How can a carrier distinguish between numbers dialed to signal another carrier's equipment and a TTY transmission providing the recipient a phone number to call?

In short, to the accessing carrier, all post-cut-through dialed digits must be treated as content and only provided to law enforcement pursuant to a wiretap order. To do otherwise would subject the carrier to liability and fail to protect the privacy of communications not otherwise authorized to be intercepted. The Commission recognizes and employs this very logic in regard to packet-mode communications, stating that CALEA's mandate to protect the privacy of communications not authorized to be intercepted

> would seem to be violated if the carrier were to give [law enforcement] both call-identifying and call content information when only the former were authorized. Under those circumstances, [law enforcement] would be receiving call content information without having the requisite authorization.[60]

---

58 47 U.S.C. § 103(b)(1).

59 18 U.S.C. § 2518(5).

60 FNPRM at ¶ 63.

There is no credible distinction between the Commission's decision in regard to packet delivery and post-cut-through dialed digits. Neither should be provided without the proper authorization.

Finally, in response to the Commission's question about how extracted digits would be delivered to law enforcement, AT&T notes that DOJ asks that the Commission require carriers to provide such information over data channels rather than content channels.[61] While DOJ recognizes that CALEA does not require this outcome, it asks the Commission to mandate it all the same.[62] AT&T continues to reject the continued efforts by law enforcement to shift the cost of CALEA to industry and asks the Commission to leave this issue to individual carrier implementations if the punch list requirement is imposed.

AT&T recognizes that law enforcement would like to avoid the trouble of getting the information from long distance or other carriers.[63] But Congress stated unequivocally that CALEA "is not intended to guarantee 'one-stop-shopping' for law enforcement."[64] By requiring dialed digit extraction, the Commission would act contrary to the intent and clear language of CALEA.

II. DISPOSITION OF JSTD-025 AND OTHER TECHNOLOGIES AND SYSTEMS

A. Remand for Amendment of JSTD-025

AT&T strongly supports the Commission's decision to remand to TIA's Subcommittee TR45.2 any additional standards development necessary to implement the Commission's final order. However, the Commission set an "ambitious" schedule of 180 days from the date of

---

61 DOJ Petition at 47.

62 *Id.*

63 DOJ Petition at 40 n. 18.

64 House Report at 3502.

release of the order to complete the amendment process.[65] AT&T believes that period of time may not be sufficient to complete an amendment to JSTD-025 through normal TIA procedures, especially because the final standard would have to undergo balloting, review, and publication. AT&T suggests that the technical amendments to JSTD-025 be complete within the 180 days as noted, but exclusive of the procedures for final promulgation as an industry standard. The Commission, of course, could assign personnel to monitor progress and require regular meeting reports to be filed by TIA to ensure that the amendment process is proceeding expeditiously.[66]

B. Commission's Role in Future Standards

The Commission also asks what role, if any, it can or should play in assisting other industry segments not covered by JSTD-025 to set standards for or to achieve compliance with CALEA.[67] The short answer is that the Commission is limited to its statutorily defined role under Section 107(b):

> Commission Authority.--If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards.[68]

Thus, unless a party asks the Commission to intercede in the standards process, it can have no direct role in future standards setting efforts.

---

65 FNPRM at ¶ 133.

66 Many of industry's representatives on the TR45.2 subcommittee also serve on other TIA standards subcommittees that are addressing such important Commission mandates as number portability and E911. Meeting schedules and locations are set months in advance and are set now well into 1999. Industry is committed to completing any amendment expeditiously, and perhaps as an alternative to an arbitrary date certain, the Commission should task the subcommittee to report a schedule after its first meeting, which the Commission could alter if it disagreed.

67 FNPRM at ¶ 141.

68 47 U.S.C. § 1006(b).

Yet, the Commission should recognize that its efforts in regard to JSTD-025 will indirectly inform future standards. That is why AT&T has argued in these comments that the Commission should announce general capability principles under Section 103, leaving it to industry associations or standard setting bodies to implement the requirements based on the particular technology. For example, rather than require that new *messages* be created to report party joins and drops in a conference call, the Commission would be better served to simply require, as a general principle, that carriers ensure dynamic reporting of known participant changes in a conference call. Then, industry experts can determine how to optimize this capability.

The failure to adopt general principles will result in future standards efforts either slavishly adhering to JSTD-025 to provide irrelevant information (e.g., all future technologies must have busy tone to report that the recipient of the call is not available whether or not there is any network utility to the signal) or designing features not articulated in JSTD-025 because they are not "covered" by CALEA. Neither is a desirable outcome and both can be avoided.

The Commission simply should make clear that the standard it pronounces as compliant for traditional voice telephony is not a "checklist" against which other standards will be judged in the future. Rather, it is one manifestation of technical requirements for circuit mode voice communications. Nothing precludes other standards from being developed -- including for voice telephony[69] -- and, unless challenged and overturned by the Commission, compliance with that standard will be a safe harbor and a complete defense to any enforcement effort by DOJ.

---

[69] There certainly could be a standard for CMRS, for example, that relied exclusively on a network-based solution rather than a switch-based one.

C. Packet-Mode Communications

The Commission has determined that the current record is insufficient to support a proposal for CALEA technical requirements for packet-mode communications.[70] There are many such services available today and under development, as the Commission recognizes, and AT&T specifically supports the Commission's conclusion that such new technologies may require "differing CALEA solutions."[71] AT&T believes that, if the Commission forbears setting packet-mode communications standards in this proceeding, industry associations will take up the issue on their own. If not, then the CALEA compliance date will serve as a spur to individual solutions.

The Commission also properly concludes that "packet data and packet-switching technology is subject to [CALEA] only to the extent it is used to provide telecommunications services, and not for information services."[72] In its prior comments, AT&T specifically requested that JSTD-025 be changed by errata to delete reference to Cellular Digital Packet Data ("CDPD") services as a telecommunications service.[73] AT&T does not repeat the rationale for the request here but incorporates its prior comments by reference and urges the

---

70 FNPRM at ¶ 64.

71 FNPRM at ¶ 64. This is particularly true with packet-mode services under development such as Internet Protocol-based cable telephony. Whether CALEA even applies to such services is an open question pending completion of the Commission's rulemaking on covered and exempt services, but it is clear that JSTD-025, with its reliance on connection-oriented communications, does not illuminate any CALEA requirements for a connectionless environment based on packet routing. Determining how to meet CALEA's requirements should be left up to the emerging cable telephony industry to define in the first instance.

72 FNPRM at ¶ 63.

73 *See* AT&T Comments at 17-22. In addition, AT&T argued that CDPD was not CMRS as defined by the Communications Act of 1934. *Id.* AT&T does not repeat this argument here but believes the Commission should address it in this or its pending rulemaking on covered carriers in order to ensure that CDPD providers will have adequate notice of their obligations under CALEA.

Commission to address this issue in its final order because it is fundamental to providing carriers notice of their CALEA obligations in regard to particular services.

III. SECTION 107(b) FACTORS

A. The Unknown Cost of the Punch List

The Commission strongly encourages specific and detailed comment on the applicability of the Section 107(b) factors to those punch list items it determined are required by CALEA.[74] Thus, the Commission asks for information regarding the costs of adding each punch list feature and what impact such costs will have on subscribers, including the costs to a manufacturer and a carrier to install and operate the equipment.[75]

AT&T joins the Commission in wanting to know that information. AWS, for example, has asked its vendors the same questions. For a variety of reasons, the information has not been forthcoming. Some vendors claim that pricing information cannot be provided until there is a stable set of punch list requirements to price.

Further, AWS's vendors will not provide pricing information on the punch list for competitive reasons without a promise of confidentiality. Thus, AWS would not, in any event, be free to share it with the Commission. Then, the vendors raise antitrust concerns

---

[74] FNPRM at ¶ 29. Specifically, Section 107(b), 47 U.S.C. § 1006(b), permits the Commission only to promulgate a rule to achieve CALEA's requirements that -

(1) meets the assistance capability requirements of section 103 by cost-effective methods;

(2) protects the privacy and security of communications not authorized to be intercepted;

(3) minimizes the cost of such compliance on residential ratepayers;

(4) serves the policy of the United States to encourage the provision of new technologies and services to the public; and

(5) provides a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

[75] FNPRM at ¶ 30.

about discussing pricing information and refuse to do so absent a DOJ opinion permitting disclosure. In short, pricing information for the punch list currently is not available at all through AT&T.

Other carriers may be in the same position and the Commission may not have a record upon which to base its decision. Whether adequate cost information is made available will not be apparent until after this first round of comments.

However, if manufacturers choose to submit the information subject to the Commission's confidentiality rules,[76] then AT&T and others will be denied an opportunity to review and comment on the cost issue, let alone to understand how the data may affect competition. It is very likely that an additional comment period will be required if the data is not disclosed in the initial comments.

B. The Cost of JSTD-025

The Commission has not acknowledged that the cost to industry of JSTD-025 is a relevant factor itself. The Commission's final rule will incorporate and amend JSTD-025. While the Commission has decided not to examine JSTD-025 from a compliance point of view in these proceedings,[77] it has no alternative but to examine its costs under Section 107(b). Unfortunately, the record may not be complete here either after the first round of comments because the Commission did not ask for comments on the cost of providing JSTD-025.

---

[76] *See* 47 C.F.R. § 0.459 (as revised by Report and Order 98-184, released July 29, 1998). While the Commission generally has not afforded confidential treatment to material submitted in rulemakings, such requests may be granted, particularly when the subject matter relates to competitively sensitive or proprietary information and could harm the party submitting the material if disclosed. *Id.* The Commission could also enter into protective agreements. Order at ¶ 43. Whether such a procedure meets Section 107(b) is an open question. Congress specifically noted that Section 107 proceedings were to be on the record and open. House Report at 3507 ("This section is also intended to add openness and accountability to the process of finding solutions to intercept problems. Any FCC decision on a standard for compliance with this bill must be made publicly.")

[77] FNPRM at ¶ 45.

For its part, AWS has received some information from its manufacturers on the cost of JSTD-025 compliance and has been able to determine additional costs for the delivery function. As the Commission knows, AWS is a national provider of wireless communications, serving 8.7 million subscribers in the United States, across a network comprised of almost 70 switches from two primary manufacturers, Ericsson and Lucent Technologies.[78] Several large urban service areas integrate switches from both vendors to provide service.[79]

Hardware and software upgrades for the basic switches, home location register, call data channel interfaces and switching circuits, in the aggregate, total over $22 million.[80] In addition, AWS's delivery functions will add over $13 million to the total. Thus, in hardware and software alone, AWS can expect to pay over $35 million just for JSTD-025 compliance.

AWS does not yet have such costs as (1) network operations costs related to the ongoing management and maintenance of the CALEA equipment;[81] (2) plant costs in addition to hardware and software such as inspecting, testing and reporting on the condition of telecommunications plant to determine the need for replacements, rearranges and changes; rearranging and changing the location of plant not retired; inspecting after modifications have been made; the costs of modifying equipment records, such as administering trunking and circuit layout work; modifying operating procedures; property held for future telecommunications use; provisioning costs; network operations costs; training to perform

---

78 If the merger with Vanguard is completed, AWS will add the Nortel switch to its network as well.

79 In a multi-switch environment, integration of switch types is critical. Yet, because of the short time frame granted by the Commission on the compliance date, AWS's vendors will not respond to AWS network requirements. Rather, AWS itself will have to undertake the integration of each of the vendor's disparate and proprietary solutions.

80 The price includes some customer discount, but the percentage cannot be disclosed.

81 AWS does know that it will incur an annual maintenance charge of $1.5 million for certain equipment that is part of the delivery function, but cannot disclose further information in that regard.

plant work; the costs of direct supervision and office support of this work;[82] or (3) General and Administrative (G&A) costs such as any management, financial, and other expenditures which are incurred by or allocated to a business unit as a whole like Accounting and Finance, External Relations, Human Resources, Information Management, Legal, Procurement.[83] AWS notes that these costs are to be incurred between now and June 2000, at a time that the company must incur other costs to meet, for example, the Commission's E911 mandates and Year 2000 compliance.

On a per switch basis for AWS, hard costs will reach almost $500,000. The other direct costs of CALEA are not insubstantial either. For example, AWS understands that not all law enforcement agencies will be CALEA-ready by June 2000 -- indeed, as AWS understands it, the government has taken no steps to contract for a collection function to receive CALEA information. AWS may have to maintain two systems of surveillance -- one using CALEA functionality and one using the current, traditional methods. It is also certain that, as with any new service, initial maintenance and operation costs will be high, including everything from personnel time to development of software patches.

Faced with these high costs, AWS alternatives under the statute are two: pass the costs on to consumers as a surveillance tax or seek relief under Section 109 of CALEA, asking the Commission to determine that compliance is not reasonably achievable. Of course, all of this is before the addition of any punch list item. Thus, the Commission should move cautiously before deciding to add to the carrier burden these enhanced features of dubious value but high cost.

---

82 Each of these items are recognized by DOJ as costs that would be recoverable if the Attorney General reimbursed a carrier for upgrading its equipment. *See* 28 C.F.R. § 100.10.

83 The Attorney General has determined that G&A costs would not be recoverable under her cost recovery rules. *Id.* Nonetheless, these are costs a carrier incurs in the implementation of CALEA.

IV. CONCLUSION

AT&T continues to support a reasonable surveillance capability and believes that JSTD-025 provides a robust and practical approach to CALEA compliance. However, AT&T does not support the addition of costly, complex or exotic surveillance features as reflected in the punch list.

Even if the Commission's tentative conclusion about certain punch list items is correct, AT&T has raised substantial doubt about whether the information is reasonably available. Rather than address reasonable availability on an ad hoc basis for each punch list item, the Commission should first decide whether the term as defined by industry in JSTD-025 is inadequate. Inasmuch as future standards setting bodies will refer to the Commission's work in these proceedings, defining reasonably available call-identifying information is perhaps the most important thing the Commission will do.

Finally, the Section 107(b) factors must be examined on the record and if the initial comments do not produce an adequate record, further proceedings will be necessary. AT&T supports a full, industry-wide review of the cost-efficacy of not only the punch list, but also JSTD-025, which by itself imposes material costs on carriers.

Respectfully submitted,

AT&T Corp.

By Seth S. Gross

Mark C. Rosenblum
Stephen C. Garavito
Seth S. Gross

AT&T Corp.
Room 3252F3
295 North Maple Avenue
Basking Ridge, New Jersey 07920
(908) 221-4432

Douglas I. Brandon
Roseanna DeMaria
AT&T Wireless Services, Inc.
Fourth Floor
1150 Connecticut Avenue
Washington, D.C. 20036
(202) 223-9222

December 14, 1998

CERTIFICATE OF SERVICE

I, Rena Martens, do hereby certify that on this 14th day of December, 1998, a copy of the foregoing "Comments of AT&T Corp. Regarding Further Notice of Proposed Rulemaking on CALEA Capabilities" was served by U.S. first class mail, postage prepaid, to the parties listed on the attached service list.

Rena Martens

Rena Martens

Service List
CC Docket No. 97-213

Pamela J. Riley
David A. Gross
AirTouch Communications, Inc.
1818 N Street, N.W.
Suite 800
Washington, D.C. 20036

Michael W. Mowery
AirTouch Communications, Inc.
2999 Oak Road, MS1025
Walnut Creek, CA 95596

Elaine Carpenter
Aliant Communications, Inc.
1440 M Street
Lincoln, NE 68508

Glenn S. Rabin
ALLTEL Corporate Services, Inc.
655 15th Street, N.W., Suite 220
Washington, D.C. 20005

Steven Shapiro
Cassidy Sehgal
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004

James P. Lucier, Jr.
Americans for Tax Reform
1320 18th Street, N.W.
Suite 200
Washington, D.C. 20036

Richard J. Metzger
Emily M. Williams
Association for Local
Telecommunications Services
888 17th Street, N.W., Suite 900
Washington, D.C. 20006

James F. Ireland
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
Attorney for Centennial Cellular Corp.

Lisa S. Dean
Center for Technology Policy
Free Congress Foundation
717 Second St., N.E.
Washington, D.C. 20002

Susan W. Smith
CenturyTel Wireless, Inc.
3505 Summerhill Road
No. 4 Summer Place
Texarkana, TX 75501

Anita Sheth
Citizens for a Sound Economy
1250 H Street, N.W.
Suite 700
Washington, D.C. 20005

David L. Sobel
Marc Rotenberg
Electronic Privacy Information Ctr.
666 Pennsylvania Ave., S.E.
Suite 301
Washington, D.C. 20003

Kurt A. Wimmer
Gerard J. Waldron
Alane C. Weixel
Covington & Burling
1201 Pennsylvania Avenue, N.W.
PO Box 7566
Washington, D.C. 20044-7566
Attorneys for EPIC, EFF, and the ACLU

Mark J. Emery
Technical Consultant (EPIC, ACLU, EFF)
3032 Jeaninnie Anna Ct.
Oak Hill, VA 20171

Catherine Wang
Swidler & Berlin
3000 K Street, N.W., Suite 300
Washington, D.C. 20007
Attorney for Ericsson Inc.

Alan R. Shark
American Mobile
Telecommunications Association, Inc.
1150 18th St., N.W., Suite 250
Washington, D.C. 20036

Barry Steinhardt
Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco, CA 94103-4832

Elizabeth R. Sachs, Esq.
Lukas, McGowan, Nace & Gutierrez
1111 19th Street, N.W., Suite 1200
Washington, D.C. 20036

Barbara J. Kern
Ameritech Corporation
Room 4H74
2000 Ameritech Center Drive
Hoffman Estates, IL 60196

John T. Scott, III
Crowell & Moring LLP
1001 Pennsylvania Ave., N.W.
Washington, D.C. 20004
Attorneys for Bell Atlantic Mobile, Inc.

Gerald W. Fikis
Bell Emergis -
Intelligent Signalling Technologies
Suite 412
78 O'Connor Street
Ottawa, ON Canada K1P 3A4

M. Robert Sutherland
Theodore R. Kingsley
BellSouth Corporation
Suite 1700
1155 Peachtree Street, N.E.
Atlanta, GA 30309-3610

Michael P. Goggin
BellSouth Cellular Corp.
Suite 910
1100 Peachtree Street, N.E.
Atlanta, GA 30309-4599

J. Lloyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N.E.
Atlanta, GA 30375

Charles M. Nalbone
BellSouth Personal Communications, Inc.
3353 Peachtree Road, N.E., Suite 400
Atlanta, GA 30326

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbridge Center Dr., 4th Fl.
Woodbridge, NJ 07095-1106

Michael Altschul
Randall S. Coleman
Cellular Telecommunications
Industry Association
1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036

Daniel J. Weitzner
James X. Dempsey
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006

Martin L. Stern
Lisa A. Leventhal
Preston Gates Ellis
& Rouvelas Meeds LLP
1735 New York Avenue, N.W.
Suite 500
Washington, D.C. 20006
Attorneys for Center for Democracy
and Technology

Andy Oram
Computer Professionals
for Social Responsibility
PO Box 717
Palo Alto, CA 94302

Louis J. Freeh, Director
Larry R. Parkinson
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

H. Michael Warren
CALEA Implementation Section
Federal Bureau of Investigation
14800 Conference Center Drive
Suite 300
Chantilly, VA 20151

Honorable Janet Reno
Stephen W. Preston
Douglas N. Letter
U.S. Department of Justice, Civil Division
601 D Street, N.W., Room 9106
Washington, D.C. 20530

John F. Raposa
Richard McKenna
GTE Service Corporation
600 Hidden Ridge, HQE03J36
PO Box 152092
Irving, TX 75015-2092

Gail L. Polivy
GTE Service Corporation
1850 M Street, N.W.
Suite 1200
Washington, D.C. 20036

James T. Roche
Timothy S. Shea
GlobeCast North America Incorporated
400 North Capitol Street, N.W.
Suite 880
Washington, D.C. 20001

Catherine Wang
Swidler & Berlin Chtd.
3000 K Street, N.W., Suite300
Washington, D.C. 20007
Attorney for ICG Telecom Group, Inc.

David L. Nace
B. Lynn F. Ratnavale
Lukas, Nace, Gutierrez & Sachs Chtd.
1111 19th Street, N.W., Suite 1200
Washington, D.C. 20036
Attorneys for Liberty Cellular, Inc., Bristol
Bay Cellular Partnership, Bristol Bay
Telephone Cooperative, Inc., and
North Carolina RSA 3 Cellular
Telephone Company

Dean L. Grayson
Lucent Technologies Inc.
1825 Eye Street, N.W.
Washington, D.C. 20006

Henry M. Rivera
Larry S. Solomon
J. Thomas Nolan
M. Tamber Christian
Ginsburg, Feldman & Bress,Chtd.
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036
Attorneys for Metricom, Inc.

Richard C. Barth
Mary E. Brooner
Motorola, Inc.
Suite 400
1350 I Street, N.W.
Washington, D.C. 20005

Stewart A. Baker
Thomas M. Barba
Maury D. Shenk
L. Benjamin Ederington
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Counsel for Motorola, Inc.

David Cosson
L. Marie Guillory
National Telephone
Cooperative Association
2626 Pennsylvania Avenue, N.W.
Washington, D.C. 20037

John Pignataro
Sr. Technical Advisor
New York Police Dept.
Ft. Totten Bldg. 610
Bayside, NY 11359

Robert S. Foosaner
Lawrence R. Krevor
Laura L. Holloway
Nextel Communications, Inc.
1450 G Street, N.W.
Suite 425
Washington, D.C. 20005

Albert Gidari
Perkins Coie
1201 Third Ave., 40th Fl.
Seattle, WA 98101
Attorney for Nextel Communications

Stephen L. Goodman
William F. Maher, Jr.
Halprin, Temple, Goodman & Sugrue
1100 New York Avenue, N.W.
Suite 650, East Tower
Washington, D.C. 20005
Attorneys for Northern Telecom Inc.

Frank X. Froncek
Northern Telecom Inc.
4001 East Chapel Hill-Nelson Highway
Research Triangle Park, NC 27709-3010

Emilio W. Cividanes
Piper & Marbury, L.L.P.
1200 19th Street, N.W.
Washington, D.C. 20036
Attorneys for Omnipoint
Communications, Inc.

Lisa M. Zaina
Stuart Polikoff
OPASTCO
21 Dupont Circle N.W.
Suite 700
Washington, D.C. 20036

Judith St. Ledger-Roty
Paul G. Madison
Kelley Drye & Warren, LLP
1200 19th Street, N.W., Suite 500
Washington, D.C. 20036
Attorneys for Paging Network, Inc.

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006
Attorneys for Personal Communications
Industry Association

Mark J. Golden
Robert Hoggarth
Personal Communications
Industry Association
500 Montgomery Street, Suite 700
Alexandria, VA 22314-1561

Jill F. Dorsey
Powertel, Inc.
1233 O.G. Skinner Drive
West Point, GA 31833

William L. Roughton, Jr.
PrimeCo Personal Communications, L.P.
601 13th Street, N.W.
Suite 320 South
Washington, D.C. 20005

Caressa D. Bennet
Dorothy E. Cukier
Bennet & Bennet, PLLC
1019 19th Street, N.W.
Suite 500
Washington, D.C. 20036
Attorneys for Rural
Telecommunications Group

James D. Ellis
Robert M. Lynch
Durward D. Dupre
Lucille M. Mates
Frank C. Magill
SBC Communications Inc.
175 E. Houston, Room 4-H-40
San Antonio, TX 78205

Robert Vitanza
SBC Communications Inc.
15660 Dallas Parkway, Suite 1300
Dallas, TX 75248

Carole C. Harris
Christine M. Gill
Anne L. Fruehauf
McDermott, Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005
Attorneys for Southern
Communications Services, Inc.

Joseph R. Assenzo
Sprint Spectrum L.P. d/b/a Sprint PCS
4900 Main St., 12th Fl.
Kansas City, MO 64112

Matthew J. Flanigan
Grant Seiffert
Telecommunications Industry Ass'n.
1201 Pennsylvania Avenue, N.W.
Suite 315
Washington, D.C. 20004

Stewart A. Baker
Thomas M. Barba
Maury D. Shenk
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Counsel for TIA

Kevin C. Gallagher
360° Communications Company
8725 W. Higgins Road
Chicago, IL 60631

Peter M. Connolly
Koteen & Naftalin
1150 Connecticut Ave., N.W.
Washington, D.C. 20036
Attorneys for United States
Cellular Corporation

Linda Kent
Keith Townsend
Lawrence E. Sarjeant
United States Telephone Association
1401 H Street N.W., Suite 600
Washington, D.C. 20005

Kathryn Marie Krause
Edward M. Chavez
Dan L. Poole
U S West, Inc.
1020 19th Street, N.W., Suite 700
Washington, D.C. 20036

William T. Lake
John H. Harwood, II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420
Attorneys for U S West, Inc.