DOCKET FILE COPY ORIGINAL

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

RECEIVED
MAY 20 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

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

To: The Commission

**COMMENTS OF THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION REGARDING THE SCOPE OF CALEA CAPABILITY REQUIREMENTS**

Michael Altschul
Vice President and General Counsel

Randall S. Coleman
Vice President
Regulatory Policy & Law

**Cellular Telecommunications Industry Association**
1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036
(202) 785-0081

May 20, 1998

No. of Copies rec'd 0+10
List A B C D E

SUMMARY 1

I. A BRIEF OVERVIEW OF THE INDUSTRY STANDARD 5

II. DOJ PUNCHLIST REQUIREMENTS ARE NOT CONSISTENT WITH CALEA 9

A. Call-Identifying Information 9

B. Additional Punchlist Items that are not Required by CALEA 16

III. REMANDING ANY NECESSARY STANDARDS DEVELOPMENT TO TR45 IS APPROPRIATE 18

IV. CONCLUSION 22

**SUMMARY**

The Cellular Telecommunications Industry Association ("CTIA") submits these Comments regarding the scope of the assistance capability requirements of Section 103 of the Communications Assistance for Law Enforcement Act ("CALEA") as requested in the Federal Communications Commission ("Commission") Public Notice dated April 20, 1998. CTIA urges the Commission to reject the broad interpretation of CALEA put forward by the Federal Bureau of Investigation ("FBI") and the Department of Justice ("DOJ"). The Commission must narrowly construe CALEA's obligations as Congress directed. Should the Commission make any changes to the industry standard that implements CALEA, CTIA supports remand to TR-45.2 to ensure technical compatibility with the existing document.

**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 THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION REGARDING THE SCOPE OF CALEA CAPABILITY REQUIREMENTS

In its Public Notice dated April 20, 1998, the Federal Communications Commission ("Commission") requested comment on the scope of the assistance capability requirements of Section 103 of the Communications Assistance for Law Enforcement Act ("CALEA").[1] In these comments, the Cellular Telecommunications Industry Association ("CTIA")[2] urges the

---

[1] Public Notice, DA 98-762, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket 97-213 (released April 20, 1998) at 4.

[2] CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the association covers all Commercial Mobile Radio Service ("CMRS") providers, including 48 of the 50 largest cellular and broadband personal

Commission to interpret the requirements of CALEA narrowly as Congress directed.

In their Joint Petition for Rulemaking, the Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI")(collectively, "DOJ") ask the Commission to adopt requirements that would force a redesign of communications networks so that their primary function will be surveillance processing rather than call processing.[3] DOJ asks for capabilities that they never before had, and information they never before received. DOJ argues for the broadest possible interpretation of CALEA's provisions and "one-stop-shopping" for all of their surveillance needs.

DOJ's extravagant demands should be rejected completely. The industry standard more than meets CALEA,[4] was developed as

---

communications service ("PCS") providers. CTIA represents more broadband PCS carriers and more cellular carriers than any other trade association.

[3] In the Matter of Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act, Department and FBI Joint Petition for Expedited Rulemaking filed March 27, 1997 [hereinafter "DOJ Petition"].

[4] The Center for Democracy and Technology ("CDT") has asked the Commission to remove location tracking from the

Congress intended through industry consensus, and is entitled to Commission deference. Indeed, before accepting DOJ's approach of looking at what the standard does not provide, the Commission should review exactly what the standard does address to implement CALEA as Congress intended.

But before doing so, CTIA offers a simple observation that is well-supported in the legislative history of CALEA and in the structure of the Act itself: CALEA was compromise legislation. CALEA was not passed to ensure that law enforcement can obtain all information from telecommunications carriers that possibly could be collected. Indeed, FBI Director Freeh testified in support of CALEA that "[t]he legislation, in our view, is not just a compromise but a

---

standard and to prohibit the delivery of the entire data packet to law enforcement on less than a wiretap order. In the Matter of Communications Assistance for Law Enforcement Act, CDT Petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed March 26, 1997 [hereinafter "CDT Petition"]. CTIA acknowledges that the standard is not the CALEA floor and that, through the process of trying to reach consensus with law enforcement, more than the minimum required by CALEA is reflected in the standard. Of course, the standard recognizes that all information can only be delivered to law enforcement when lawfully authorized, but this is different than saying that CALEA requires certain information to be provided or to be withheld.

victory for all of the interests involved. The legislation reflects reasonableness in every provision."[5]

In fashioning the compromise that became CALEA, Congress warned all parties with CALEA obligations, including law enforcement, the Commission and the telecommunications industry, to interpret the law's requirements narrowly:

> The Committee urges against overbroad interpretation of the requirements. The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.[6]

Thus, for each of DOJ's punchlist items the Commission should ask (1) whether the capability is expressly provided for in CALEA; (2) if not, whether the capability was addressed in the legislative history; and (3) if not, whether the

---

[5] *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*, 103rd Cong., 2d Sess., 113 (1994) (Testimony of FBI Director Freeh).

capability is consistent with a narrow interpretation of the statutory section upon which DOJ bases its claim. Conversely, when the Commission reviews J-STD-025, it should ask (1) is the capability provided for in CALEA; (2) if so, is it narrowly tailored to preserve the delicate balance between law enforcement's electronic surveillance needs and privacy protections as reflected in the legislative history.

CTIA is confident that the Commission, upon reviewing the standard, will find all of the statutory mandates answered. In reviewing the DOJ punchlist, the Commission will find only a wish list of enhanced capabilities not reflected in the statute at all.

## I. A BRIEF OVERVIEW OF THE INDUSTRY STANDARD

J-STD-025 defines the interfaces between a telecommunications carrier and a law enforcement agency to assist that agency in conducting lawfully authorized electronic surveillance. The purpose of the standard was to facilitate compliance with the assistance capability requirements of Section 103 of CALEA and to help ensure efficient and industry-wide implementation of CALEA's

---

[6] H. Rep. No. 103-837, at 23, *reprinted in* 1994

requirements. The standard was developed as a joint standards project between American National Standards Institute-accredited Telecommunications Industry Association Committee TR-45 and Committee T-1-Telecommunications.

In essence, the standard provides the means to enable law enforcement access to the content of a subscriber's communications and to related call-identifying information. Call-identifying information is formatted into discrete messages using a special protocol. These messages are delivered over a call data channel ("CDC") separate from the call content channel ("CCC").

Call-identifying information messages inform law enforcement that a party has answered a call attempt (answer message); the system has routed a call dialed by the subscriber or the system has translated a number for the subscriber (origination message); a call has been redirected, forwarded, diverted or deflected (redirection message); the facilities for the entire call have been released (release message) and a call attempt to the subscriber has been detected (termination attempt message). In addition, messages are provided to report the beginning and end of call content

---

U.S.C.C.A.N. 3489, 3502-03 [hereinafter "House Report"].

delivery and any change in the call identities when calls are split or merged. Finally, there is also a message to report when a mobile subscriber is authorized for service on another system.

J-STD-025 uses the precise CALEA definition for call-identifying information and 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).[7]

The standard provides for access to all communications to or from a subscriber's equipment, facilities or services. The standard provides that loss of any call content should not occur between call completion and call release, and indeed, that call content may be delivered before answer (which includes call progress tones and any recorded announcements).

---

[7] J-STD-025, Section 3.0, Definitions.

A multi-party communication is accessed as well as it would be presented to the subscriber.[8]

The standard provides for association of call content and call identifying information through the use of time stamps, call identity parameters, and assignment of case identities. The call identity parameter allows the messages to be associated with one or more specific CCC.

In sum, the standard as written and now before the Commission is a comprehensive set of surveillance features that more than meet CALEA's requirements. For example, voice calls will be identified as they always have been - by their directory number - and advanced calling features such as call

---

[8] Law enforcement complains in its petition that it does not receive the content of communications of parties to a subscriber-initiated conference call when the subscriber places the conference on hold to answer an incoming call. However, the standard provides that a circuit intercept access point shall access a multi-party call "as it would be presented to" the subscriber. J-STD-025, Section 4.5.1. Nothing in the standard precludes the delivery of the communications on the held portion of a conference call should the subscriber place the call on hold. Concern was expressed during prior consultations with law enforcement that monitoring the held portion of a conference call when the person named in the warrant is not present may present constitutional questions. The standard would allow for an implementation where the content is not delivered if the carrier determines that it is not lawfully authorized.

forwarding will not thwart surveillance because law enforcement will receive all of the content of redirected calls. This is precisely what Congress intended.

## II. DOJ PUNCHLIST REQUIREMENTS ARE NOT CONSISTENT WITH CALEA

### A. Call-Identifying Information

Three of DOJ's punchlist items depend completely on the Commission accepting a "broad definition of call-identifying information in CALEA."[9] A telecommunications carrier must expeditiously isolate call-identifying information reasonably available to the carrier and enable the government to access it.[10] 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.[11]

---

[9] DOJ Petition at 34.

[10] 47 U.S.C. § 1002(a)(2).

[11] 47 U.S.C. § 1001(2).

As noted above, J-STD-025 employs the exact statutory definition.[12] The standard then gives further definition to the terms "origin, direction, destination, or termination" based upon the accepted understanding of these terms in the industry. The standard defines them 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).[13]

The Commission will find that these definitions track carefully the use of the terms in the statute and in the legislative history. For example, Congress stated that for voice communications, "call-identifying information" is "the numbers dialed or otherwise transmitted for the purpose of routing calls through the carrier's network."[14]

---

[12] J-STD-025, Section 3.0, Definitions.

[13] *Id.*

[14] House Report at 3501.

Further, in pen register cases, Congress stated that call-identifying information is "the numbers dialed from the facility that is the subject of the court order."[15] For trap and trace investigations, call-identifying information is "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."[16]

DOJ would have the Commission include three additional features as "call-identifying," but as the Commission will note, there are many more features under each heading than just three. DOJ asks for *all* subject-initiated dialing and signaling; (2) the creation of new messages to advise when a party is placed on hold, drops or joins a call; and (3) notification of network-generated in-band and out-of band signals. For each of these, the Commission should refer back to the basic questions -- where in CALEA or its legislative history is this requirement found, and is it consistent with a narrow interpretation of the law.

---

[15] *Id.*

[16] *Id.*

### (a) Subject-initiated dialing and signaling

Law enforcement contends that flash hooks and feature keys that place a party on hold are call-identifying information. DOJ characterizes this information as signaling, and they are correct. But DOJ fails to note that only signaling that identifies the "origin, direction, destination or termination of a call" is covered by CALEA. Flash hooks or other feature keys do not identify anything, and therefore are not call-identifying information.

DOJ also includes post-cut-through dialed digits in this category.[17] This issue is addressed in CALEA expressly. CALEA requires law enforcement to use technology reasonably available to it to restrict the recording of or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing.[18]

Indeed, in the legislative history, Congress expressly stated that "[o]ther dialing tones that may be generated by

---

[17] DOJ Petition at 38-42.

[18] 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.

the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information."[19] Indeed, FBI Director Freeh testified to Congress that he had no interest in 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.[20]

DOJ argues, however, that some post-cut-through dialed digits actually do route calls such as long distance services through use of an 800 number. There is no dispute that the accessing carrier must provide law enforcement, as the standard requires, the 800 number dialed by the subscriber and

---

[19] House Report at 3501.

[20] *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*, 103rd Cong., 2d Sess., 50 (1994) (Testimony of FBI Director Freeh).

any translation of that number that is reasonably available to the carrier.

As to post-cut-through digits, however, the accessing carrier views the call as completed. It cannot determine whether the numbers entered after the call has been completed are for purposes of completing a long distance call or controlling customer premises equipment. Law enforcement wants all of the digits, not just those that identify a post-cut-through dialed call.[21] This can hardly be viewed as a narrow interpretation of CALEA and must be rejected.[22]

**(b) Party hold, drop and join messages**

DOJ also asks the Commission to mandate that carriers create a specific, new set of messages to identify whenever a subscriber places a call on hold or a party to conference call

---

[21] In any event, the numbers that direct the call are provided on another carrier's equipment, facilities or services, not those of the subscriber's system which is covered by CALEA.

[22] Carriers that provide post-cut-through information after October 25, 1998, may face claims that they fail to protect the privacy of communications not authorized to be intercepted. 47 U.S.C. § 1002(b)(3).

joins or drops.[23] This is information that DOJ never received before.[24]

Only by stretching the definition of call-identifying information can DOJ make an argument that this information is call-identifying. There is no dispute that DOJ receives the number of each party joined in the conference call under the standard. If the law enforcement agency has provisioned enough lines, it will hear the conversations as they occur. If the case is a pen register, then they already have the numbers dialed to identify the parties to a call.

They are missing nothing other than the opportunity to infer again for some hypothetical case that a target was on a particular conference call when material discussions of a crime occurred. This is exactly the status quo.

**(c) Network-generated in-band and out-of band signaling**

There is nothing in CALEA that requires carriers to provide law enforcement with signaling that "can be sensed by

---

[23] DOJ Petition at 42.

the subject."[25] Once again, in making their argument, DOJ fails to link the signal to the origin, direction, destination or termination of a call. How a network treats a call is not call-identifying in any meaningful sense of the word.[26]

The Commission should reject all of the punchlist items based on the attenuated DOJ definition of call-identifying information. The standard treats such information consistent with the intent of Congress and the words of the statute. No change or addition is warranted.

### B. Additional Punchlist Items that are not Required by CALEA

The same set of CTIA questions apply to the additional punchlist items, which actually go to how carriers do business, maintain their networks, and interface with law enforcement. DOJ seeks to "automate" the relationship, with carriers paying the price for this enhanced service. For example, DOJ asks the Commission to require electronic

---

[24] 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.")

[25] DOJ Petition at 47.

[26] DOJ Petition at 46.

notification that a carrier's equipment is functioning through an "automated delivery of surveillance status information."[27]

Similarly, DOJ also wants an "automated" feature status message to be informed whenever a subscriber adds or drops services.[28] Apparently, the traditional subpoena method simply is too slow or cumbersome for law enforcement, so they would have carriers automate it at their own expense.

DOJ also seeks to insert timing and correlation requirements for delivery of messages and association of those messages with intercepted call content. CALEA does not specify a delivery time for messages.[29] CALEA specifies no timing requirements at all. The standard properly leaves the issue to carrier implementation.

---

[27] DOJ Petition at 52.

[28] DOJ Petition at 56.

[29] DOJ Petition at 51.

## III. REMANDING ANY NECESSARY STANDARDS DEVELOPMENT TO TR45 IS APPROPRIATE

CTIA continues to support remand to TIA's Subcommittee TR45.2 of any necessary standards development.[30] As the Commission notes, this Subcommittee developed the J-STD-025 and therefore is uniquely positioned to ensure that any changes required by the Commission are integrated consistently and properly.[31]

DOJ has urged the Commission to move forward with the implementation of J-STD-025, but also to ensure that such development is forward-compatible with any punchlist items the Commission might decide are required.[32] While CTIA and DOJ disagree on what action the Commission should take on any industry-wide extension, CTIA agrees that the Commission must

---

[30] Public Notice at 4. *See also* In the Matter of Rulemaking Under Section 1006 of the Communications Act of 1934, as Amended, and Section 107 of the Communications Assistance for Law Enforcement Act to Resolve Technical Issues and Establish a New Compliance Schedule, TIA Petition for Rulemaking filed April 2, 1997; *and* Response to Petition for Rulemaking by CTIA, the Personal Communications Industry Association and the United States Telephone Association, filed April 9, 1998 ("Joint Industry Response".

[31] Public Notice at 4.

ensure that any changes it directs, whether by addition or deletion of capabilities, integrate with the industry standard. The best and most efficient way for that to occur is by remand to the Subcommittee that drafted the standard in the first place.

The Commission has not asked for technical comments on the proposed DOJ rule. While CTIA provides some critique in these Comments, the Commission should understand that industry does not accept the technical merit of the DOJ proposal. To the contrary, CTIA has prepared a brief set of technical comments on the proposal,[33] and no doubt other associations, manufacturers and carriers will have comments as well. The Commission should not put itself in the position of attempting to resolve differing technical comments. The consensus-based, standards-setting process is designed and well-suited for such a process, which underscores the desirability of remanding any change in the standard to TR45.2.

---

[32] *See* DOJ Reply Comments Regarding the Commission's Authority to Extend the October 25, 1998 Compliance Date at 13.

[33] *See* Declaration of Kirk Carlson, Exhibit 1 (commenting on the DOJ proposed rule).

This fact is evidenced by the progress of the Enhanced Surveillance Services ("ESS") project. As the Commission knows, CTIA urged the creation of the ESS standards project in order to provide the law enforcement customer with enhanced surveillance features that, although outside CALEA, could otherwise be lawfully authorized.[34]

The ESS has met three times to date and initially projected completion of a standard in less than 18 months. However, law enforcement has not contributed to the process in good faith. Indeed, they have not even presented their proposed rule for consideration. But through the give and take of the meetings, law enforcement has admitted that some of its requests to the Commission are not well-articulated or even required any longer (such as separated delivery of call content and a limited set of delivery protocols).[35] The Commission need only peruse the enclosures to the letter to understand the need to remand any change in the standard.

---

[34] Nothing in the creation of the ESS should suggest that CTIA believes any of the punchlist items are technically or reasonably achievable. Only time will tell once the capabilities have been vetted through the standards process and vendors begin development efforts.

As the Joint Industry Response noted, the Commission has the authority to remand any changes in the standard to TR45.2 for final implementation, even where Congress empowers the Commission by statute to promulgate such rules itself.[36] CALEA itself recognized the appropriateness and lawful of a delegation to industry standard-setting organizations so long as the policy is clearly articulated.[37]

CTIA strongly supports leaving the administration of the standard in the hands of industry itself. This will ensure that future revisions that may be necessary due to changing technology or the introduction of new services will be facilitated in accordance with well-established revision procedures, rather than by petition to the Commission for a rule change. Such an approach also will ensure that a process for vetting such changes from an industry perspective will be available.

---

[35] *See* P. Musgrove, Chair, TR-45.2 ESS Ad Hoc, letter dated to Mike Warren, CIS, attached as Exhibit 2.

[36] Joint Industry Response at 12 (citing *In the Matter of Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings; Implementation of Sections 551(c), (d), and (e) of the Telecommunications Act of 1996*, ET Docket No. 97-206 (released Mar. 13, 1998)).

Accordingly, CTIA supports remand of any changes the Commission deems necessary to TR45.2.

## IV. CONCLUSION

CTIA urges the Commission to reject the additional capabilities proffered by DOJ and to acknowledge the industry standard as a safe harbor for carriers. Should the Commission require any modifications to the standard, those changes should be accomplished through TIA's TR45.2 Subcommittee.

Respectfully submitted,

Michael Altschul
Vice President and General Counsel

Randall S. Coleman
Vice President
Regulatory Policy & Law

**Cellular Telecommunications Industry Association**
1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036
(202) 785-0081

May 20, 1998

---

[37] House Report at 3506-07.