Summary of CALEA Requirements

1 References

[1] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in 18 U.S.C. ⁄ 2522, and 47 U.S.C.⁄⁄ 229, 1001-1010.) http://www.techlawjournal.com/agencies/calea/47usc1001.htm.

[2] H.R. Rept. 103-827 PART 1. 103RD CONGRESS 2d Session.[1] http://www.epic.org/privacy/wiretap/calea/H_Rpt_103_827.txt.

[3] FCC 97-356, cc Docket No. 97-213, Notice of Proposed Rulemaking, released 10/10/97. *http://wireless.fcc.gov/csinfo/calea.html. Document identified by release date.*

[4] FCC 98-223, cc Docket No 97-213 Memorandum Opinion and Order, released 9/11/98. *http://wireless.fcc.gov/csinfo/calea.html. Document identified by release date.*

[5] FCC 98-282, cc Docket No. 97-213 Further Notice of Proposed Rulemaking, released 11/5/98. *http://wireless.fcc.gov/csinfo/calea.html. Document identified by release date.*

[6] FCC 99-011 cc Docket No. 97-213 Report and Order, released 3/15/99. *http://wireless.fcc.gov/csinfo/calea.html. Document identified by release date.*

[7] FCC 99-229, cc Docket No. 97-213 Second Report and Order, released 8/31/99. *http://wireless.fcc.gov/csinfo/calea.html. Document identified by release date.*

[8] FCC 99-230, cc Docket No. 97-213, Third Report and Order, released 8/31/99. *http://wireless.fcc.gov/csinfo/calea.html. Document identified by release date.*

[9] ANSI J-STD-025, Lawfully Authorized Electronic Surveillance, published December 19, 2000.

[10] U.S. Court of Appeals for the District of Columbia Circuit, United States Telecom Association, et al., Petitioners, v. Federal Communications Commission and United States of America, Respondents, August 15, 2000. http://www.epic.org/calea/

1. *House of Representatives Report together with additional views to accompany CALEA. The legislative history is an interpretive tool used to understand the statutory text.*

dc_cir_decision.html.

[11] United States Code, Title 18--Crimes And Criminal Procedure. *http://wais.access.gpo.gov*.

2 Acronyms

CALEA: *Communications Assistance for Law Enforcement Act.*

FCC: *Federal Communications Commission, US.*

HR: *House of Representatives, US.*

LEA: *Law Enforcement Agencies.*

NPRM: *FCC Notice of Proposed Rulemaking.*

18 USC: *Title 18 United States Code.*

LAES: *Lawfully Authorized Electronic Surveillance.*[2]

2. [9] at 8.

3 Introduction

This document provides information in the form of quotations and discussions regarding Communications Assistance for Law Enforcement Act (CALEA) legal requirements. The quotations are drawn from various sources including CALEA itself, FCC orders, J-STD-025, and the House of Representatives congressional report to accompany CALEA. It is the hope of TR45 LAES Ad Hoc that this information will be of value to the Standards Development Organizations developing lawful intercept standards for packet mode technologies to meet CALEA obligations for such technologies.

The House of Representatives Report gives the scope of CALEA. FCC 99-230 cc Docket No. 97-213, released after consideration by the FCC of filings on provacy concerns, refer to this scope (nested quote) and to the need to protect provacy interests:

"CALEA, enacted on October 25, 1994, was intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently in the face of rapid advances in telecommunications technology. In enacting this statute, however, Congress recognized the need to protect privacy interests within the context of court-authorized electronic surveillance. Thus, in defining the terms and requirements of the Act, Congress sought to balance three important policies: '(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.'[3][4]

Note: for the reader's convenience, quotes are in plain text and discussion is in italicized text.

3. [2] at 13.

4. [8] at ¶ 2.

4 Definitions from CALEA

Communications Assistance for Law Enforcement Act, sec. 102 Definitions.

4.1 Call-identifying information

"The term 'call-identifying information' means 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."[5]

4.2 Electronic messaging service

"The term 'electronic messaging services' means software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages."[6]

4.3 Information service

"The term 'information services'--

(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

(B) includes--

(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;

(ii) electronic publishing; and

(iii) electronic messaging services; but

(C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network."[7]

5. [1] at sec.102.
6. id.
7. id.

4.4 Telecommunications support service

"The term 'telecommunications support services' means a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunications network."[8]

4.5 Telecommunications carrier (Telecommunications Service Provider)

"The term 'telecommunications carrier'--

(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and

(B) includes--

(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))); or

(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title; but

(C) does not include--

(i) persons or entities insofar as they are engaged in providing information services; and

(ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General."[9]

8. [1] at sec.102.

9. id.

5 Definitions from Title 18 United States Code

5.1 Content

"when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."[10]

5.2 Electronic communications

"any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."[11]

5.3 Pen register

"a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."[12]

5.4 Trap and Trace

"a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication".[13]

10. [11] at sec. 2510 (8).
11. id. at sec. 2510 (12).
12. id. at sec. 3127 (3).
13. id. at sec. 3127 (4).

6 Definitions and assumptions from the FCC

6.1 Content of subject-initiated conference calls

"Capability that permits a[n] LEA to monitor the content of conversations by all parties connected via a conference call when the facilities under surveillance maintain a circuit connection to the call."[14]

6.2 Location

"... in the wireless (cellular or broadband PCS) environment ... the location of the cell site to which the mobile terminal or handset is connected at the beginning and at the termination of the call."[15]

6.3 Packet mode

" A communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s)."[16]

"We [FCC] recognize that call identifying information for packet technologies also may be acquired from the carrier's records".[17]

6.4 Timing Information

"...capability that permits a[n] LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event timestamped to an accuracy of at least 200 milliseconds."[18]

14. [8] at sec. VI. Appendix A: Final Rules §§ 22.1102, 24.902 and 64.2202.
15. id. at ¶ 45.
16. [9] at 9.
17. id. at ¶ 55 footnote 107.
18. [8] at sec. VI. Appendix A: Final Rules §§ 22.1102, 24.902 and 64.2202.

7 Definitions and Assumptions from J-STD-025

The following definitions and assumptions are from J-STD-025, Section 3 (Definitions and Acronyms) or Section 4.2.1 (Assumptions).

7.1 Associate

"A telecommunication user whose equipment, facilities, or services are communicating with a subject."[19]

7.2 Call-identifying information

"Defined in CALEA Section 102 (2) to be '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 [TSP].' As interpreted by this standard: **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)."[20]

"Call-identifying information is reasonably available if the information is present at an Intercept Access Point (IAP) for call processing purposes. With respect to the matters before the FCC the commission has provided the following additional guidance: call-identifying information is 'reasonably available' to a TSP if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications. 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 reasonable available at an IAP may vary between different technologies and may change as technology evolves."[21] (footnote omitted.)

7.3 Communication

"Communication refers to any wire or electronic communication as defined in 18 USC 2510."[22]

19. [9] at chapter 3.
20. id.
21. id. at chapter 4, sec 4.2.1.
22. id. at chapter 3.

7.4 Intercept subject

"a telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity)."[23]

7.5 Packet-mode

"a communication where individual packets or virtual circuits of a communication within a physical circuit are switched or routed by the accessing telecommunication system. Each packet may take a different route through the intervening network(s)."[24]

7.6 Unobtrusive

"not undesirably noticeable or blatant; inconspicuous; within normal call variances."[25]

23. [9] at chapter 3.

24. id.

25. id.

8 CALEA requirements[26]

"To insure that law enforcement can continue to conduct wiretaps."[27]

8.1 SEC. 103. ASSISTANCE CAPABILITY REQUIREMENTS

"Capability Requirements. -- Except as provided in subsections (b)"[28] "(c)"[29] "and (d)"[30] "'of section 103 and sections 108(a)"[31] "and 109(b)"[32] "and (d)"[33], "a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of--"[34]

8.1.1 Intercept communications

"expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic 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, or at such later time as may be acceptable to the government;"[35]

8.1.2 Access call-identifying information

"expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely

26. [1] at sec.103.
27. [2] at 16. Legislation.
28. [1] at sec.103(b) Limitations.
29. id. at sec.103(c) Emergency or Exigent Circumstances.
30. id. at sec.103(d) Mobile Service Assistance Requirements.
31. id. at sec.108(a) Grounds for Issuance.
32. id. at sec.109(b) Equipment, Facilities, and Services Deployed on or Before January 1, 1995.
33. id. at sec.109(d) Failure to Make Payment With Respect To Equipment, Facilities, and Services Deployed on or Before January 1, 1995.
34. id. at sec. 103(a).
35. id. at sec. 103(a)(1).

pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);"[36]

8.1.3 Deliver information and communications to law enforcement

"delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and"[37]

8.1.4 Provide privacy and unobtrusive interception

"facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information."[38]

8.1.5 Provide mobile service assistance

"Mobile Service Assistance Requirement.- A telecommunications carrier that is a provider of commercial mobile service (as defined in section 332(d) of the Communications Act of 1934) offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of a wire or electronic communication service that has acquired access to the communications."[39]

36. [1] at sec. 103(a)(2).

37. id. at sec. 103(a)(3).

38. id. at sec. 103(a)(4).

39. id. at sec. 103(d).

8.1.6 Decryption capability

"Encryption.-A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[40]

8.1.7 Monitoring on TSP premise during emergency

"Emergency or Exigent Circumstances.- In emergency or exigent circumstances (including those described in sections 2518 (7) or (11)(b) and 3125 of title 18, United States Code, and section 1805(e) of title 50 of such Code), a carrier at its discretion may comply with subsection [103](a)(3)[Delivery of communication to law enforcement] by allowing monitoring at its premises if that is the only means of accomplishing the interception or access."[41]

8.1.8 Specific industry design is not required

"This title does not authorize any law enforcement agency or officer-- (A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services."[42]

8.1.9 Industry change is not prohibited

"This title does not authorize any law enforcement agency or officer-- (B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services."[43]

8.2 Compliance with CALEA assistance capability requirement under accepted standards

"Although CALEA does not specify technologies or standards that carriers must use to meet the assistance capability requirements, it does contain a 'safe harbor' provision. . ."[44]

40. [1] at sec. 103(b)(3).
41. id. at sec. 103(c).
42. id. at sec. 103(b)(1).
43. id.
44. [4] at ¶ 4.

"Compliance under accepted standards - A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to set the requirements of section 103."[45]

8.3 Alternative compliance with CALEA capability requirements

"It is important to make clear the distinction between technology and equipment that is 'CALEA-compliant' and equipment that is compliant with TIA's interim standard [J-STD-025]. The term CALEA-compliant technology refers to any technology that could be used to meet the assistance capability requirements of section 103 of CALEA--whether it adheres to the interim standard or not. Technology solutions based on the interim standard are thus just one way for a carrier to comply with CALEA's requirements."[46]

"...because J-STD-025 is a voluntary standard, we [FCC] believe that forcing carriers through a forbearance agreement to pledge that they will develop and use equipment meeting J-STD-025 specifications might arguably go beyond what Congress intended, thus undermining the use of the standard as a safe harbor, and effectively nullifying the technical flexibility Congress sought to preserve in sections 103(b)(1) and 107(a)."[47]

"We [FCC] note ... that individual carriers are free to choose any technical solution that meets the assistance capability requirements of CALEA, whether based on an industry standard or not. Carriers, therefore, have some degree of flexibility in deciding how they will comply with CALEA's section 103 requirements. See H.R.Rep. No.103-827, 103rd Congress, 2d Sess, pt. 1, at 3507 (1994) ('Compliance with the industry standard is voluntary not compulsory. Carriers can adopt other solutions for complying with the capability requirements.')."[48]

"... However, compliance with CALEA's capability requirements is still required even if a carrier chooses not to use publicly available standards. [49] In that case, the carrier would have to work with its equipment suppliers to develop and deploy an alternative technical solution(s) that would meet the capability requirements."[50]

45. [1] at sec. (107)(a)(2).
46. [4] at footnote 40.
47. id. at ¶ 27.
48. [8] at footnote 7.
49. original footnote 14 references [1] at sec.107(a)(3)(B).
50. [4] at ¶ 4.

8.4 Telecommunication Service Provider Security and Integrity

"A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission."[51]

"Therefore, CALEA prohibits law enforcement agencies from remotely activating interceptions within a carrier's switching premises. Under CALEA, all interceptions require the intervention and cooperation of a designated and authorized carrier officer or employee."[52]

8.5 Consultation with industry

"Consultation. - To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representatives of users of telecommunications equipment, facilities, and services, and with State utility commissions."[53] (Footnoes omitted)

51. [1] at sec. 105.

52. [3] at ¶ 21 and [6] for further information.

53. [1] at sec. 107(a)(1).

9 CALEA does not have requirements for:[54]

"Information services; private networks and interconnection services and facilities.- The requirements of subsection [103](a) do not apply to (A) information services".

9.1 Information services

"(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and (B) includes - (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services."[55]

"The term 'information services' includes messaging services offered through software such as groupware and enterprise or personal messaging software, that is, services based on products (including but not limited to multimedia software) of which Lotus Notes (and Lotus Network Notes), Microsoft Exchange Server, Novell Netware, CC: Mail, MCI Mail, ... and AT&T Easylink (and associated services) are both examples and precursors. It is the Committee's intention not to limit the definition of 'information services' to such current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of 'information services'. By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill."[56]

"The legislative history of CALEA makes clear that the requirements of CALEA do not necessarily apply to all offerings of a carrier. The House Report states: '[C]arriers are required to comply only with respect to services or facilities that provide a customer or subscriber with the ability to originate, terminate, or direct communications.'[57] We [FCC] therefore find that an entity is a telecommunications carrier subject to CALEA to the extent it offers, and with respect to, such services."[58]

9.2 Private networks and interconnection services

"... equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers."[59]

54. [1] at sec 103(b)(2).
55. id at sec. 102(6).
56. [2] at 21.
57. original footnote 26 references [2] at 21.
58. [7] at ¶ 11.

"...CALEA does not apply to private network services: [T]elecommunications services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers...need not meet any wiretap standards. PBXs are excluded. So are automated teller machine (ATM) networks and other closed networks. Also excluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line."[60]

59. [1] at sec.103(b)(2)(B).

60. [7] at ¶ 12.

10 FCC Requirements

Below is information taken from the FCC notices, reports, and orders.

The list of requirements from FCC 99-230 cc Docket No. 97-213 includes those that have not been vacated and remanded to the FCC by the United States Court of Appeals for the District of Columbia Circuit No. 99-1442 decided August 15, 2000. The four requirements that have been vacated and remanded, as described in J-STD-025 are: 'conference party change/ connection/connection break', 'subject signal', 'network signal', and 'dialed digit extraction.' The FCC terminology for these four vacated requirements are: 'Party hold, hoin, drop', 'Subject-initiated dialing and signaling inforamtion', 'In-band and out-of-band signaling'. and 'dialed digit extraction'.

10.1 Packet mode

"...We [FCC] are aware that packet-mode technology is rapidly changing, and that different technologies may require differing CALEA solution for separating call-identifying information from call content. We also recognize that we must avoid implementing CALEA requirements that could impede the development of new technologies..."[61]

"...We [FCC] believe that further efforts can be made [in J-STD-025] to find ways to better protect privacy by providing law enforcement only with the information to which it is lawfully entitled...."[62]

10.1.1 Background and discussion

"The Further NPRM noted that packet data and packet-switching technology are potentially usable for both information services and telecommunications services, but that such technology is subject to CALEA requirements only to the extent it is used to provide telecommunications services, and not for information services. The Further NPRM also noted that privacy concerns could be implicated if carriers were to give to LEAs packets containing both call-identifying and call content information when only the former was authorized...."[63]

"We [FCC] find that the approach taken with regard to packet-mode communications in J-STD-025 raises significant technical and privacy concerns. ... We are aware that packet-mode technology is rapidly changing, and that different technologies may require differing CALEA solutions for separating call-identifying information from call content. We also recognize that we must avoid implementing CALEA requirements that could impede the development of new technologies. We do not believe that the record sufficiently

61. [8] at ¶ 55.

62. id.

63. id. at ¶ 48.

addresses packet technologies and the problems that they may present for CALEA purposes. For example, some packet technologies (e.g., frame relay, ATM, X.25) are connection oriented--i.e., there are call set-up and take-down processes, similar to those used in circuit switched voice networks, whereby addressing information is made available to the carrier separate from and before call content is transmitted. Other packet technologies (e.g., internet protocol based solutions) would not be processed this way. We believe that further efforts can be made o find ways to better protect privacy by providing law enforcement only with the informaiton to which it is lawfully entitled. We note that TIA recomments further sudy of the matter. Accordingly, we invite TIA to study CALEA solutions for packet-mode technology and report tot he Commission in one year on steps that can be taken, including particular amendments to J-STD-025, that will better address privacy concerns. In the interim, we find that packet-mode communications, including call-identifying information and call content, may be delivered to law enforcement under the interim standard.[64] Further, we are herein requiring that packet-mode communications be delivered to LEAs under that standard no later than September 30, 2001. That date is 15 months after the June 30, 2000 CALEA compliance deadline, and will afford manufacturers that have not yet developed a packet-mode capability the time needed to do so."[65]

10.2 Timing Information

"Capability that permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event timestamped to an accuracy of at least 200 milliseconds."[66]

10.2.1 Background

"Specifically, because we [FCC] find it to be a reasonable compromise between the DoJ/FBI and TIA proposals, we will adopt the DoJ/FBI proposal that the event be defined as the time the call-identifying information is received at the IAP and TIA's proposal that this information, including a time stamp, be transmitted to the LEA's Collection Function within eight seconds 95% of the time, and that the time stamp be accurate within 200 milliseconds. We find that TIA's proposal to define the event as the time the call-identifying message is detected by the Delivery Function to be insufficient because in some circumstances this message might not be detected by the Delivery Function until well after it was received at the IAP. However, we find the DoJ/FBI proposal for delivery of the message from the IAP to the LEA's Collection function within 3 seconds 99% of the time with 100 millisecond accuracy to be overly stringent and possibly excessively costly to carriers given the various network designs used by carriers in different services

64. [8] at ¶ 55 original footnote 107 "We [FCC] recognize that call identifying information for packet technologies also may be acquired from the carrier's records."

65. id. at ¶ 55.

66. [8] at section VI. Appendix A: Final Rules § 22.1102, §§ 22.902, and 64.2202.

applying this requirement. Accordingly, we will require that delivery of a call-identifying message be transmitted to the LEA's Collection Function within eight seconds of its receipt by the IAP 95% of the time, and with an accuracy within 200 milliseconds."[67]

10.3 Content of subject-initiated conference calls

"Capability that permits an LEA to monitor the content of conversations by all parties connected via a conference call when the facilities under surveillance maintain a circuit connection to the call."[68]

10.3.1 Background

"...When the subject puts the conference call on hold, the subject's circuit to the conference call is maintained within the carrier's network (usually at the subscriber's serving switch), thus allowing the subject to rejoin easily the call without having to reinitiate the circuit. In this case, we [FCC] find that the communication continues to or from the equipment, facility or service of the subscriber, and thus the carrier also must provide the content of the communication among the other parties to the conference call.... however, we conclude that the carrier does not have to provide access to the content of the communication between a participant of the conference call other than the subject and any person with whom that participant speaks on an alternative line...."[69]

"We [FCC] reach a different conclusion when the subject terminates his circuit connection to the conference call. In this case, the communication between other participants no longer is to or from the subscriber's equipment, facilities, and services, and may no longer even be "carried by the carrier within a service area" to or from the subscriber of the carrier, pursuant to section 103(a) and (d).[70] This is especially true with conference bridges located in remote switches of other carriers. We conclude that it is not reasonable to require the carrier to provide at its IAP the communications of other parties continuing on the conference call after the subject terminates his circuit connection to the call because to do so would not be a cost-effective method of implementing the conference call intercept and may not protect the privacy and security of communications not authorized to be intercepted, pursuant to section 107(b).[71] We recognize, as DoJ/FBI acknowledge, that if the subject arranges for a "meet me" conference bridge, the LEA will need a [separate] Title III order to cover the communication of the conference

67. [8] at ¶ 96.

68. id. at section VI. Appendix A: Final Rules § 22.1102, §§ 22.902, and 64.2202..

69. id. at ¶ 66.

70. id. at ¶ 67 original footnote 128 "Section 103(d) requires that when a commercial mobile service carrier conducting a lawful interception of wire and electronic communications loses 'access to the content of such communications or call-identifying information within the service area ..., information is made available to the government ... identifying the provider of a wire or electronic communication service that has acquired access to the communications'".

bridge. Under those circumstances, the carrier that provides the conference bridge should provide an IAP to the LEA."[72]

10.4 Location

"We [FCC] also note that the equivalent location information in the wireless (cellular or broadband PCS) environment appears to be the location of the cell sites to which the mobile terminal or handset is connected at the beginning and at the termination of the call...."[73] "We will not, however, mandate a location tracking capability in this proceeding.... We believe that a more generalized capability that will identify only the location of a cell site, and only at the beginning and termination of the call, will give LEAs adequate information....Accordingly, as had been agreed to by both DoJ/FBI and the telecommunications industry, we mandate a location capability that will identify cell site location at the beginning and termination of a call."[74]

71. [8] at ¶ 67 original footnote 129 "We [FCC] recognize that some multi-party calls may be bridged within the subscriber's serving switch, and thus may continue to be within the service area, pursuant to section 103 (a) and (d). Nonetheless, we will not require a carrier to provide the communications of other parties continuing on the call after the subject terminates his connection because to do so may not protect the privacy and security of communications not authorized to be intercepted."

72. id. at ¶ 67.

73. id. at ¶ 45.

74. id. at ¶ 46.

10.5 Capabilities must fall within the provisions of CALEA

The Third Report and Order released, August 31, 1999, discussed three messages requested by law enforcement due to alleged deficiencies in J-STD-025. The FCC devised a test to determine if messages are within CALEA and after applying the test (described in the following paragraph) to all three messages (the Feature Status message, the Surveillance Status message, and the Continuity Check Tone message) determined they did not meet CALEA and therefore are not required.

The FCC test states that to be required under CALEA, the information such a feature would provide would identify the 'origin, direction, destination , or termination' of each communication (e.g., call-identifying information), or be required under section 103(a), the assistance capability requirements.

- *(1) expeditiously isolating the content of targeted communications transmitted by the carrier within its service areas;*
- *(2) expeditiously isolating information identifying the origin and destination of targeted communications;*
- *(3) transmitting intercepted communication and call-identifying information to law enforcement agencies at locations away from the carrier's premises; and*
- *(4) carrying out intercepts unobtrusively, so that targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications).*

10.5.1 Surveillance Status message

"Discussion: CALEA requires carriers to ensure that authorized wiretaps can be performed in an expeditious manner, and we [FCC] believe that a surveillance status message could assist carriers and LEAs in determining the status of such wiretaps. We conclude, however, that a surveillance status message does not fall within any of the provisions of section 103. We do not believe that it is call-identifying information as defined by CALEA, since the information such a feature would provide would not identify 'the origin, direction, destination, or termination of each communication.' Nor does a surveillance status message appear to be required under section 103(a)(1), since it is not a wire or electronic communications carried on a carrier's system. Nor are we persuaded by the FBI's interpretation that a surveillance status message is required by CALEA's direction that a carrier 'shall ensure' that its system is capable of meeting the section 103 (a) requirements. Rather, we note that the Act expressly states 'a telecommunications carrier shall ensure that its equipment, facilities, or services.... are capable of' intercepting communications and allowing LEA access to call identifying information. We interpret the plain language of the statue to mandate compliance with the capability requirements of section 103(a) but not to require that such capability be proven or verified on a continual basis. Ensuring that a wiretap is operational can be done in either a technical or non-technical manner, and section 103(a) does not include 'ensurance' as a capability. Thus we conclude that the surveillance status punch list item is not an assistance capability requirement under section 103..."[75] (Footnotes omitted.)

10.5.2 Continuity Check Tone message

"...the plain language of the statue mandates compliance with the capability requirements of section 103(a), but does not require that such capability be proven or verified on a continual basis.... Thus (as with the case of surveillance status messages) we [FCC] conclude that the continuity check tone punch list item is not an assistance capability requirement under section 103, nor does it fall within CALEA's definition of call-identifying information"....[76]

10.5.3 Feature Status message

"This technical requirement would require a carrier to notify the LEA when specific subscription-based calling services are added to or deleted from the facilities under surveillance, including when the subject modifies capabilities remotely through another phone or through an operator. Examples of such services are call waiting, call hold, three-way calling, conference calling, and call return.[77] Also the carrier would be required to notify the LEA if the telephone number of the facilities under surveillance was changed or service was disconnected...." [78]

"...First we [FCC] believe it is clear that feature status messages do not constitute call-identifying information since the information such a feature would provide would not identify 'the origin, direction, destination, or termination of each communication'....Further, feature status messages do not appear to be required under section 103(a)(1) because they are not wire or electronic communications carried on a carrier's system....We reiterate that the plain language of the Act mandates compliance with the assistance capability requirements of section 103(a). but does not require carriers to implement any specific quality control capabilities to assist law enforcement. The information sought by DoJ/FBI in a feature status message can be provided in either a technical or non-technical manner, and section 103(a) does not include 'ensurance' itself as a capability....[79]

75. [8] at ¶ 101.

76. id. at ¶ 106.

77. id. at ¶ 107 footnote 209. "We [FCC] note that some services, such as call return, are available on either a subscription or per-call basis. DoJ/FBI assert, however, that the availability of per-call features is irrelevant to their petition and that they do not seek to require carriers to notify a[n] LEA of a subscriber's use of these features. They explained that carriers should simply alert a[n] LEA to the assignment or removal of features that can affect call content or call-identifying information from a line under surveillance. They conclude that, '[a]s a practical matter, law enforcement will know in advance what per-call features a particular carrier makes available to its subscribers, and will have collected enough information to predict the...likely use of such features, before initiating an intercept, and will be able to order the appropriate number of call content and call data channels based on this information'..."

78. id. at ¶ 107.

79. id. at ¶ 111.