

STEPTOE & JOHNSON LLP

ATTORNEYS AT LAW

ORIGINAL

1330 Connecticut Avenue, NW
Washington, DC 20036-1795

Telephone 202.429.3000
Facsimile 202.429.3902
www.steptoel.com

Thomas M. Barba
202.429.8127
tbarba@steptoel.com

EX PARTE OR LATE FILED

RECEIVED

DEC - 3 1999

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

December 3, 1999

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

EX PARTE NOTICE

**Re: In the Matter of Communications Assistance for Law
Enforcement Act, CC Docket No. 97-213**

Dear Ms. Salas:

On December 2, 1999, the Cellular Telecommunications Industry Association ("CTIA"), represented by Michael Altschul, Tom Barba and Ben Ederington, met with Susan Kimmel, Stacy Jordan, and John Spencer (of the Wireless Telecommunications Bureau) and David Ward (of the Common Carrier Bureau) regarding this proceeding.

The discussion concerned the implementation of the Commission's *Report and Order*, CC Docket No. 97-213, FCC 99-11 (rel. March 15, 1999) on carrier security procedures, including the content and timing of statements that carriers are required to file with the Commission.

Pursuant to 47 C.F.R. § 1.1206, an original and one copy of this letter are enclosed for filing. Please do not hesitate to contact me if you have any questions.

Sincerely,



Thomas M. Barba

encl.
cc: Susan Kimmel, Stacy Jordan, John Spencer and David Ward

No. of Copies rec'd 01
List ABCDE

CONFIDENTIAL DOCUMENT FILED UNDER SEAL

[REDACTED]

December 2, 1999

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: CONFIDENTIAL DOCUMENTS FILED UNDER SEAL
CC Docket No. 97-213, [REDACTED]

[REDACTED]

Dear Ms. Salas:

Enclosed please find an original and one copy of [REDACTED] Policies and Procedures for Conducting Lawfully Authorized Electronic Surveillance. These policies and procedures are being submitted in compliance with § 64.2105 of the Commission's Rules, 47 C.F.R. § 64.2105.

This response is being submitted under seal. The response contains sensitive information (including the name and contact information for [REDACTED] principal point of contact with law enforcement). Accordingly, this submission should be treated pursuant to Section 0.459 of the Commission's Rules and should not be placed in the Commission's Public File.

If you have any questions regarding this submission, please do not hesitate to contact me at [REDACTED]. I appreciate your assistance.

Sincerely,

[REDACTED]

III. POINT OF CONTACT DUTIES

[REDACTED]

The point of contact shall ensure that no electronic surveillance is activated without first receiving appropriate legal authorization. As defined above, appropriate legal authorization means: (a) a court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications or (b) other authorization, pursuant to 18 U.S.C. 2518(7), or any other relevant federal or state statute.

Upon receipt of a proffered authorization by law enforcement, the authorization shall be reviewed to ensure it is what it purports to be (e.g., a wiretap order) and that it can be implemented technically, including that the legal authorization is sufficiently and accurately detailed to enable compliance with its terms.

The point of contact shall ensure that a record of all electronic surveillance is maintained in accordance with these Procedures. The point of contact, or the point of contact's designee, shall certify that each record of electronic surveillance is complete and accurate in accordance with these Procedures.

The point of contact shall be responsible for ensuring that all employees with electronic surveillance responsibilities are properly trained in these Procedures and are apprised of electronic surveillance requirements.

In addition to any other job functions, each point of contact shall be available 7 days a week, 24 hours a day, to implement authorized electronic surveillance. The point of contact shall ensure that electronic surveillance and technical assistance is implemented promptly as lawfully authorized.

IV. UNAUTHORIZED INTERCEPTION OR ACCESS PROHIBITED

Unauthorized interception of communications or access to call-identifying information is strictly prohibited. The point of contact shall report to the appropriate law enforcement agencies, within a reasonable time upon discovery: (a) any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities and (b) any act of unlawful electronic surveillance that occurs on [REDACTED] premises.

V. RECORDKEEPING AND CERTIFICATION

The point of contact, or the point of contact's designee, shall maintain secure and accurate records of all interceptions of communications or access to call-identifying information, made with or without appropriate authorization, in the form of a single certification. This

certification shall include the following information and shall be prepared for each surveillance performed:

- (1) the telephone number(s) and/or circuit identification numbers involved;
- (2) the start date and time of the opening of the circuit for law enforcement;
- (3) the identity of the law enforcement officer presenting the appropriate legal authorization;
- (4) the name of the person signing the appropriate legal authorization;
- (5) the type of electronic surveillance (e.g., pen register, trap and trace, Title III, FISA); and
- (6) the name of the employee responsible for overseeing the electronic surveillance and who is acting in accordance with these Procedures.

Each certification will be signed by the person overseeing the surveillance, thereby attesting that the record is accurate and complete. The certification will be completed contemporaneously with, or within a reasonable period of time after, the initiation of the electronic surveillance.

The certification requirement may be satisfied if the individual responsible for overseeing the electronic surveillance signs the certification and appends the appropriate legal authorization as well as any extension authorizations to the certification. However, the appropriate legal authorization must contain all of the information enumerated above.

Records of electronic surveillance shall be maintained, in a secure manner, for [REDACTED].

VI. SUBMISSION AND AMENDMENT OF PROCEDURES

Amendments to these Procedures must be filed with the Commission within 90 days. These Procedures must also be filed with the Commission within 90 days of the effective date of any merger or divestiture.

**TELECOMMUNICATION CARRIER CHECKLIST UNDER SECTION 105 OF THE
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (“CALEA”)**

The Federal Communications Commission has adopted regulations¹ under Section 105 of CALEA to ensure that telecommunication carriers have policies and procedures in place for effectuating lawful interceptions through their switching premises.

These regulations require telecommunication carriers to:

- Appoint a senior officer or employee as “Point of Contact” responsible for ensuring that interception of communication or electronic surveillance can only be activated with proper authorization.
- Revise internal policies and procedures to provide:
 - A point of contact job description;
 - A method of enabling law enforcement authorities to contact the designated point of contact around-the clock, seven days a week; and
 - An interpretation of the phrase “appropriate authorization” (that encompasses the FCC’s definitions of “appropriate legal authorization” and “appropriate carrier authorization”).
 - *Appropriate legal authorization* means: “(1) a court order signed by a judge or magistrate authorizing or approving interception of wire or electronic communications; or (2) other authorization, pursuant to 18 U.S.C. § 2518(7), or any other federal or state statute.”
 - *Appropriate carrier authorization* means: “the policies and procedures adopted by telecommunications carriers to supervise and control officers and employees authorized to assist law enforcement in conducting any interception of communications or access to call-identifying information.”
 - A statement that carrier employees must receive “appropriate authorization” before enabling the interception of communications or access to call-identifying information.

¹ In the Matter of Communications Assistance for Law Enforcement Act, *Report and Order*, CC Docket No. 97-213 (rel. Mar. 15, 1999), *modified by* In the Matter of Communications Assistance for Law Enforcement Act, *Order on Reconsideration*, CC Docket No. 97-213 (rel. Aug. 2, 1999).

- A detailed description of how long it will maintain its records of each interception of communications or access to call-identifying information. (see below; the period must be a “reasonable period of time”).
- Report compromises of security and unlawful interceptions of communications or access to call-identifying information to the appropriate law enforcement officials “within a reasonable length of time upon discovery.”
- Maintain a secure and accurate record of each interception of communications or access to call-identifying information, made with or without appropriate authorization, in the form of single certifications.
 - A certification must be compiled either contemporaneously with, or in a reasonable time after, the initiation of the interception or the surveillance.
 - An individual certification must be prepared for each surveillance performed.
 - These certifications must be retained for a “reasonable period of time” (as identified by the carrier’s policies and procedures).
 - Each certification shall include, at minimum, the following information:
 - The telephone number(s) and/or circuit identification numbers involved;
 - The start date of the opening of the circuit for law enforcement;
 - The identity of the law enforcement officer presenting the authorization;
 - The name of the person signing the appropriate legal authorization;
 - The type of interception of communications or access to call-identifying information;
 - The name of the telecommunications carriers’ personnel who is responsible for overseeing the interception of communications or access to call-identifying information; and
 - The signature of the telecommunications carriers’ personnel who is responsible for overseeing the interception of communications or access to call-identifying information. This individual will, by his/her signature, certify that the record is complete and accurate.
 - Alternatively, the certification requirement may be satisfied if the individual responsible for overseeing the electronic surveillance signs the certification and appends the appropriate authorization and any extension authorizations to the

certificate, as long as the appropriate legal authorization contains all of the information listed above.

- File, within 90 days of the effective date of the rules (i.e., by March 21, 1999), or within 90 days of a carrier's merger or divestiture or a carrier's amendment of its existing policies and procedures, the policies and procedures it uses to comply with the new requirements.