and CALEA, the FBI would require carriers to build the capability to monitor all parties to a multi-party call even after the subject of the intercept order is no longer participating in the call. The purpose of CALEA was to follow the target, not to facilitate monitoring of those left behind after the subject of the court order is no longer on the call. The FBI is seeking the capability to monitor the held portion of a conference call even when it is known that the subject is on another call entirely. Not only is this not mandated by CALEA, but providing it would violate section 103(a)(4)(A), since law enforcement is not authorized to intercept the calls of people not named in the order, when they are not using the facilities named in the order.

(2) In-band digits that the subject dials after cut-through -- When a person uses a long distance calling card, he or she first dials the 800 or local number that leads to the long distance carrier's system. The local carrier treats this as a completed call and establishes a content channel for the calling party. Then the caller is prompted by the long distance carrier to dial additional numbers, including the desired ultimate destination of the long-distance toll call. To the system of the local exchange carrier complying with a surveillance order, these digits dialed after call cut-through do not identify a call. By definition, they are "post cut-through." This means that for the carrier complying with the order, the call has been properly routed and any further dialed digits are treated as indistinguishable from other content. Law enforcement wishing to intercept these post cut-through digits has two choices: serve the first carrier with a content interception order, or serve the long-distance carrier, which does treat the digits as call-routing information, with a pen register order.

The FBI does not want to make this choice. It wants the first carrier to provide the post cut-through digits under the much weaker pen register standard. First of all, these digits are not call-identifying data under the CALEA definition. The legislative history for CALEA states. "Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." H.R. Rep. 103-827, Part 1, at 21.

Second, even if the post-cut through digits were considered to be call-identifying data, they are not "reasonably available" to the local carrier on a signaling channel. CALEA section 103(a)(3) only requires carriers to provide "reasonably available" call-identifying information.

The issue here, contrary to some suggestions of law enforcement, is not the loss of post cut-through dialed digits. That information is of course available to law enforcement on the content channel with appropriate authorization or from the target's long distance carrier. The issue is whether the FBI can use CALEA to reduce the standard for access to information that carriers treat as content.

(3) Notification when the subject is signaled by the subject's services (e.g., message waiting indicator). This network intelligence does not identify a call and is outside the scope of CALEA.

(4) Party hold, drop and join messages to indicate the status of parties to a call. These messages do not relate to call-identifying information but rather seek to enhance law enforcement investigative techniques beyond the status quo.

(5) "Flash hooks and feature key usage." -- The FBI wants companies to include on the data or call-identifying channel these other elements of information, which do not fit within the definition of "call-identifying information" in CALEA.

(6) Feature Status Message -- The FBI seeks to insert a feature status message that would be activated whenever a subject's services are changed by a carrier in response to a routine administrative request or otherwise. A subject may request a change of services by mail or with

a call from a facility not under authorized surveillance. Requiring the carrier to send a message to law enforcement on the target's line whenever services are altered in response to a customer request would require companies to digitize customer information and make it available over the data channel. This would be a significant precedent -- requiring carriers to generate a type of on-line customer service profile solely for the benefit of government surveillance. This information currently is provided by subpoena and can continue to be provided in that manner. There is no basis in CALEA for requiring telecommunications carriers to add this information to their signaling channels.

By items (3) through (6), the FBI is seeking to increase the amount of information that it obtains under the minimal standard applicable to pen registers. But CALEA established a new rule for dialing and signaling information. Congress changed the authority to conduct pen registers, in a way that eliminated the provision of signaling information that does relate to call processing. Congress imposed on industry and law enforcement a new requirement: to the extent technologically possible, pen register information should be limited to dialing and signaling information used in call processing. 18 U.S.C. ß3121(c). See also 18 U.S.C. 3127(3), which defines a pen register as a device collecting "electronic or other impulses which identify the numbers dialed or otherwise transmitted." This simple phrasing in the pen register statute dovetails completely with CALEA's definition of call-identifying information. Other signaling or sounds that do not relate to dialed numbers are neither encompassed by the pen register law nor required by CALEA.

Currently, law enforcement receives information through pen registers (or the more sophisticated "dialed number recorders) that is outside the pen register statute. The fact that hook flashes, for example, are recorded today does not mean that the pen register statute or CALEA mandate that they be reported in a digital environment in response to a pen register order. Indeed, if the technology allows them to be filtered out, CALEA requires that they not be provided to the government, for they are not authorized to be intercepted.

This is not a situation where law enforcement will be denied any evidentiary data. The only question is the standard for legal access. The FBI is trying to use CALEA to move more data into the category of "call-identifying" data so that it can be available under the pen register standard. Congress clearly rejected this approach. In fact, Congress was so concerned that it choose a "belt-and-suspenders" approach. It required carriers to protect information not authorized to be intercepted and it required law enforcement agencies to use pen register devices that only recorded dialing information used in call processing.

VI. COMPLIANCE WITH THE INTERIM STANDARD IS NOT REASONABLY ACHIEVABLE

Compliance with CALEA is not reasonably achievable with respect to equipment, facilities and services installed or deployed after January 1, 1995, for the simple reason that carriers have had to make changes to their systems not knowing what was required to comply with CALEA. They still don't know, and they continue to make upgrades that compound the problem. Carriers will be in a better position than CDT to explain to the Commission how much equipment facilities and services have been installed or deployed since January 1, 1995, and what would be the cost of retrofitting that equipment to make it compliant with any reading of the statute.

But the reason why compliance is not reasonably achievable is directly related to the reason why we have filed this petition: Compliance is not reasonably achievable because the FBI has sought, in contravention of Congress' intent, a 100% foolproof surveillance system intended to address any and every aspect of law enforcement interception that could conceivably arise under present-day technology. Rather than focus on the few narrow problems that law

enforcement identified to the Congress in 1994, the FBI has promoted a comprehensive redesign of the handling of calls for the maximization of surveillance potential. The FBI and other law enforcement agencies had extensive involvement in this process -- involvement that went well beyond the "consultation" contemplated by CALEA and amounted to an attempt to dominate the process. The FBI has consistently endeavored to require that industry meet a wish-list of surveillance capability needs never contemplated by Congress. Industry rewrote its standard in many respects to accommodate the FBI's positions. As a result of these concessions, the interim industry standard already goes too far in enhancing the surveillance powers of the government and fails to protect the privacy and security of communications not authorized to be intercepted, and therefore violates CALEA. Moreover, the delay in producing this comprehensive standard has prevented the timely development of a standard that is reasonably achievable.

The FBI was reluctant to pursue "band-aid solutions." But the results have been gridlock, delay, threats to privacy and increased financial costs. It is now clear that CALEA will only be implemented -- if it can be implemented at all -- with a strict focus on preserving a core surveillance capability, rather than maximizing the surveillance potential of the digital technology.

Section 109(b) of CALEA authorizes the Commission to find compliance not reasonably achievable for equipment, facilities or services installed after January 1, 1995. (Equipment installed before January 1, 1995 does not have to be brought into compliance unless the Attorney General pays the full cost of retrofitting.) While section 107 specifies that extensions of the October 25, 1998 compliance deadline may be granted for two years, Congress was foresightful in adding the separate section 109(b) authority. Section 109 does not set any limit on how long the Commission may extend its finding that compliance not reasonably achievable. Given the extraordinary delays that have occurred, the Commission should find that all equipment deployed after January 1, 1995, including equipment deployed after October 25, 1998, cannot be reasonably brought into compliance until questions about the scope of the law are resolved. Then, considering all the factors specified in subsection 109(b)(1)(A) - (K), the Commission can set appropriate compliance timetables.

This is where the Commission's section 107 and section 109 authorities intersect. Until the interpretation of CALEA is vastly scaled back, compliance will never be reasonably achievable. While the FBI has argued with industry over the last increments of surveillance enhancements in traditional wireline and wireless systems, entirely new systems have been developed and deployed. Unless the FBI's interpretation of CALEA is vastly scaled back, this process of section 109 determinations will be never ending.

In sum, compliance is not reasonably achievable because the FBI has sought to use CALEA to enhance its surveillance capabilities. The restoration of the principle of privacy as one of the three goals of the statute is necessary if compliance is ever to be reasonably achievable. The Commission, when it remands the standard to industry, shall direct it to focus on the basic features that were raised by the FBI in 1994 - call forwarding, speed dialing, call waiting and conference calling (to ensure they do not interfere with surveillance of the target) and access to call-identifying information, narrowly construed.

VII. THE COMMISSION HAS THE AUTHORITY AND AN OBLIGATION TO OVERSEE CALEA IMPLEMENTATION

Congress clearly intended the Commission to have a role in overseeing, and if necessary deciding, the privacy issues posed by CALEA. Section 107 of CALEA states:

"If industry associations or standard-setting organizations fail to issue technical requirements

or standards or if 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 or requirements or standards that ...

(2) protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. 1006 (emphasis added).

This role for the Commission was obviously an important part of the structure that Congress intended to create in adopting CALEA. The report of the House Judiciary Committee on CALEA states:

"H.R. 4922 includes provisions, which the FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill --...

4. Allows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements, and provides that one factor for judging those standards is whether they protect the privacy of communications not authorized to be intercepted." H.R. Rep 103-827, Part 1, 17-18.

Section 109 of CALEA also gives the Commission sufficient authority to address the issues raised here:

"The Commission, on petition from a telecommunications carrier or any other interested person, and after notice to the Attorney General, shall determine whether compliance with the assistance capability requirements of section 103 is reasonably achievable with respect to any equipment, facility or service installed or deployed after January 1, 1995. . . . In making such determination, the Commission shall . . . consider the following factors:

(C) The need to protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. 1008(b)(1) (emphasis added).

CONCLUSION

Congress intended that CALEA would preserve but not expand government surveillance capabilities. The interim industry standard already goes too far. Location information is outside the mandate of CALEA. The treatment of packet switching information violates the requirement to protect the privacy and security of information not authorized to be intercepted. We urge the Commission to

(1) determine that the location tracking and packet switching provisions in the interim industry standard violate CALEA;

(2) develop a standard that suitably protects the privacy of communications not authorized to be intercepted in a packet-switched environment;

(3) reject any requests by the FBI or other agencies to further expand the surveillance capabilities of the Nation's telecommunications systems;

(4) remand the development of a CALEA standard to the appropriate industry bodies, with directions to narrow the interim standard to focus on the specific problems of call forwarding, speed and voice dialing, prompt access to dialing information, and the effects of call waiting and conference calling on the surveillance of targeted individuals, or pare back the standard itself, to the same end; and

(5) find compliance not reasonably achievable and indefinitely delay implementation of the statute, while a narrowly-focused standard is being developed.

Respectfully submitted,

Jerry Berman

James X. Dempsey

CENTER FOR DEMOCRACY AND TECHNOLOGY

1634 Eye Street, N. W. Suite 1100

Washington, DC 20006

(202) 637-9800 March 26, 1998

FOOTNOTES

1. Public Law No. 103-414, codified at 47 U.S.C. ßß 1001 - 1010 and in various sections of Title 18 and Title 47.

2. 63 Fed. Reg. 12,218 (Mar. 12, 1998), http://www.fbi.gov/calea/calea1.htm.

3. DOJ, FBI, "Communication Assistance For Law Enforcement Act, Implementation Report" (Jan. 26, 1998), available at http://www.cdt.org/digi_tele/CALEAimpjan98.html.

4. The location issues raised here are very different from those previously considered by the Commission in its proceeding on E911 services. In the 911 context, the caller presumptively consents to being located when he or she calls 911. See DOJ, Office of Legal Counsel, "Memorandum Opinion for John C. Keeney," (Sept. 10, 1996) (concluding that a person, "by dialing 911, has impliedly consented to" disclosure of his or her location). Other wireless callers do not give consent to be located, so the providing of this information poses privacy issues.

[Other CALEA Issues]

FEB 3 1998

Washington, D.C. 20530

Mr. Thomas Wheeler
President and CEO
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, NW, Suite 200
Washington, DC 20036

Dear Mr. Wheeler:

This letter confirms discussions held between the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and representatives of the telecommunications industry during a January 23, 1998, meeting[1] regarding DOJ's position on the legal status under the Communications Assistance for Law Enforcement Act (CALEA) of the 11 electronic surveillance capabilities (referred to as the "punch list") that are missing from the current Telecommunications Industry Association (TIA) electronic surveillance standard J-STD-025. Additionally, it confirms the terms and conditions upon which DOJ will forbear bringing enforcement actions against industry members for non-compliance with CALEA.

"Punch List"

DOJ has reviewed the 11 "punch list" capabilities in reference to CALEA, its legislative history, and the underlying electronic surveillance statutes[2]. In addition, DOJ reviewed a memorandum evaluating the "punch list" under CALEA that was prepared by the Office of General Counsel (OGC) of the FBI. As a result of its review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within

---

[1]Those in attendance at the January 23, 1998, meeting included representatives from the Cellular Telecommunications Industry Association (CTIA), Personal Communications Industry Association (PCIA), Telecommunications Industry Association (TIA), United States Telephone Association (USTA), Bell Atlantic, Department of Justice and the Federal Bureau of Investigation.

[2] CALEA was enacted to preserve the electronic surveillance capabilities of law enforcement commensurate with the legal authority found in the underlying electronic surveillance statues, and so that electronic surveillance efforts could be conducted properly pursuant to these statues.

review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within the scope of CALEA and the underlying electronic surveillance statutes. These nine capabilities are[3]:

- Content of conferenced calls;
- Party Hold, Party Join, Party Drop;
- Access to subject-initiated dialing and signaling;
- Notification Message (in-band and out-of-band signaling);
- Timing to correlate call data and call content;
- Surveillance Status Message;
- Feature Status Message;
- Continuity Check; and
- Post cut-through dialing and signaling.

With respect to the first four capabilities (Content of conferenced calls; Party Hold, Party Join, Party Drop; Access to subject-initiated dialing and signaling; and Notification Message of in-band and out-of-band signaling), DOJ firmly believes that law enforcement's analysis and position regarding these assistance capability requirements satisfy CALEA section 103 requirements. These descriptions are set forth in the response submitted by the FBI[4] to TIA Committee TR45.2 during the balloting process on standards document SP-3580A.

With respect to the fifth through the ninth capabilities (Timing to correlate call data and call content; Surveillance Status Message; Feature Status Message; Continuity Check; and Post cut-through dialing and signaling), DOJ has also concluded that law enforcement's position satisfies CALEA section 103 requirements. Because of this opinion, discussion between the industry and law enforcement will be required in order to select a mutually acceptable means of delivering the information specified by each capability. Thus, if industry disagrees with law enforcement's proposed delivery method, it must affirmatively propose a meaningful and effective alternative.

Based upon the foregoing analysis, it is DOJ's opinion that TIA interim standard J-STD-025 is failing to include and properly address the nine capabilities listed above. Industry and law enforcement may wish to act in concert to revise the interim standard J-STD-025 to include solutions for each of these missing electronic surveillance capabilities.

---

[3] *See* Items 1-7, 9, and 10 of Attachment A.

[4] The FBI is closely coordinating its efforts with state and local law enforcement representatives across the nation. In this document "law enforcement" and "FBI" refer to this partnership and are used interchangeably.

With respect to capability number eight (Standardized Delivery Interface), although a single delivery interface is not mandated by CALEA, DOJ believes that a single, standard interface would be cost effective and of great benefit to both law enforcement and telecommunications carriers. Recent productive discussions with industry have resulted in what DOJ believes is an acceptable compromise, whereby the industry would commit to a limited number of no more than five delivery interfaces. DOJ supports such an agreement.

With respect to capability number 11 (Separated Delivery), DOJ, while recognizing the usefulness of such delivery for the effectiveness of electronic surveillance, nevertheless does not believe that CALEA section 103, or the underlying electronic surveillance statutes, require separated delivery.

Building on the progress made during the final months of 1997, the FBI's CALEA Implementation Section (CIS) will continue to work with solution providers[5] to reach an agreement on the technical feasibility of all the CALEA capability requirements.

Forbearance

During the January 23, 1998, meeting, the parties discussed the conditions under which DOJ would agree not to pursue enforcement actions against the carrier under section 108 of CALEA with regard to the CALEA mandate that a carrier meet the assistance capability requirements pursuant to CALEA section 103 by October 25, 1998, or against a manufacturer with respect to its obligation under CALEA section 106(b) to make features or modifications available on a "reasonably timely basis." A letter from the Office of the Attorney General, which was provided to all meeting attendees, outlined the basic conditions regarding forbearance:

> In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, DOJ will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. DOJ

---

[5] Solutions providers include not only switch-based manufacturers, and support service providers, but other industry entities that are engaged in the development of network-based and other CALEA-compliant solutions.

will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement.

DOJ, in consultation with the FBI, has further elaborated on the conditions related to forbearance as follows:

Any member of the telecommunications industry seeking forbearance must submit to CIS a statement that identifies the following:

1. The CALEA capability requirements that will be included in its platform or designed into any non-switch-based solution.

2. The projected date by which the platform, or non-switch-based solution, will be made commercially available, the "commercially available date."

3. A timeline for design, development, and testing milestones that will be achieved by the manufacturer from the start of the project through the commercially available date, the "milestone timeline."

4. A schedule for furnishing information to CIS at each milestone to permit CIS to verify that a milestone has been reached.

5. A list of specific types of information to be provided according to the foregoing schedule.

6. A schedule for providing mutually agreed upon data to CIS from which the Government will be able to determine the fairness and reasonableness of the CALEA solution price.

7. A list of the specific types of price-related data to be provided.

With respect to item 1, the term "CALEA capability requirements" refers to the functions defined in the TIA interim standard J-STD-025 and the first nine punch list capabilities described earlier in this letter. Law enforcement will work with each solution provider as it produces a technical feasibility study to confirm its understanding of, and ability to meet, the CALEA capability requirements. For those switching platforms, or non-switch-based solutions, on which a capability is technically infeasible, law enforcement will consult with solution providers to assess the possibility of providing effective technical alternatives that will still provide law enforcement with the necessary evidentiary and minimization data sought by the capability.

With respect to item 2, the term "commercially available date" refers to the date when the platform or non-switch-based solution

will be made available by the solution provider for the immediate purchase and deployment by a carrier. That date shall, in no event, extend beyond the first currently scheduled software generic product release after the October 25, 1998, capability compliance date. With respect to item 3, the term "milestone timeline" refers to a schedule of the necessary design, development, and testing steps to be taken by a solution provider in making a product commercially available. With respect to item 4, a solution provider is expected to include a schedule specifying the time after the completion of each milestone when CIS will be able to verify that the milestone has been reached. With respect to item 5, the specific types of information contained in the affirmative confirmation of the foregoing schedule will include, but not be limited to, draft design documents, feature specification documents, and test results. With respect to item 6, a solution provider is expected to provide a schedule detailing the delivery to CIS of all necessary information for the government to make a determination of the fairness and reasonableness of the price of the solution provider's commercially available CALEA solution. With respect to item 7, the specific types of information contained in the price-related information of the foregoing schedule will include, but not be limited to, market prices of comparable features with similar levels of design, development, and testing effort.

Forbearance for a solution provider, and its carrier customers, will be conditioned upon its ability to provide the above listed items as well as to meet verifiable solution development milestones. A solution provider's failure to meet these milestones will result in the loss of forbearance for the solution provider.

Carrier forbearance ends with the commercial availability of a solution. Switches, or portions of a network, of historical importance to law enforcement for which the government must reimburse the carrier will be identified by CIS. Equipment, facilities, and services installed or deployed after January 1, 1995, will be included in any forbearance until a solution is commercially available. Following solution availability, for those switches or portions of a network not identified by CIS, carriers are expected to follow their normal deployment processes in determining which switches, or portions of their networks, will be upgraded with the CALEA capabilities. Figure 1 illustrates the basic elements of forbearance.

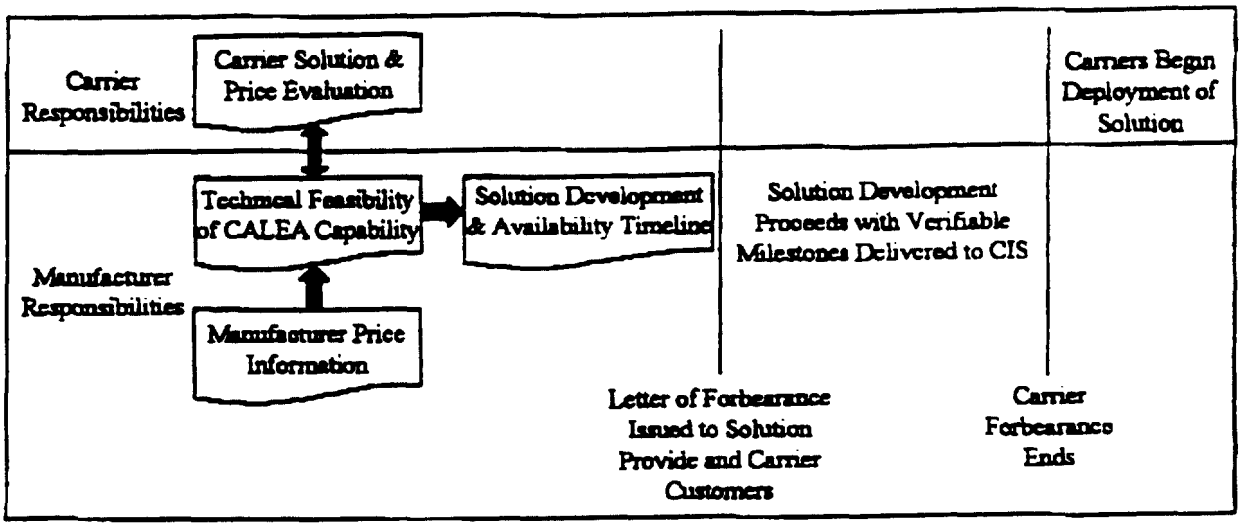

Figure 1: Forbearance

The foregoing forbearance discussion centers on two separate and distinct agreements: Agreements in Principle (AIP) between the FBI and a solution provider, and Cooperative Agreements between the FBI and a carrier.

In an AIP, the FBI and solution providers agree that solution providers have complied with the seven criteria listed above, including a feasibility analysis and pricing information for CALEA capability requirements. The feasibility analysis and pricing information will allow the government to finalize its position regarding the standard, extension of the compliance dates, forbearance, etc. The FBI, in consultation with law enforcement, will not be in a position to make critical determinations until the information described in the above seven criteria has been provided.

Currently many versions of draft AIPs are circulating, both FBI- and industry-generated, and some are more comprehensive than is presently warranted. Some of the AIPs in circulation were derived from an AIP drafted by TIA. The FBI hopes to meet with TIA during the week of February 2, 1998, to discuss the proposed AIP. The results of these discussions will then be disseminated to TIA's membership and any other interested solution provider.

The Cooperative Agreement, on the other hand, is the contractual vehicle whereby telecommunications carriers will receive reimbursement for their eligible CALEA costs. Cooperative Agreements may be executed for different purposes at different stages of CALEA implementation. For example, an initial round of Cooperative Agreement negotiations is taking place to establish contractual vehicles whereby carriers selected to support specific solution providers with the feasibility analyses and pricing information may receive reimbursement for assisting in

this effort. Unfortunately, this initial round of negotiations has encountered some problems. One of the issues is the clarification of a carrier's role in assisting in the analysis of the solution provider's proposed solution. It appears from discussions with carriers that a mutual understanding of the intent of the government's proposed language for the Cooperative Agreements and its Statement of Work (SOW) does not yet exist. Carriers commented that the SOW included a consultative role that the carriers are unable or unwilling to perform. Although it was the government's intent to construct an SOW flexible enough to allow carriers to accommodate their normal roles in the solution provider product development process, the proposals received in response to the SOW have been too non-specific to provide real value.

The FBI still believes, and has had it confirmed by solution providers, that carriers have an essential role to play in developing the CALEA solution. The FBI will now request that each solution provider describe in detail the typical interaction it might have with one of its carrier customers during new product development. These descriptions will then be incorporated into the proposed SOWs, which the government will seek from carriers.

Your continued willingness to work with law enforcement toward the development of electronic surveillance solutions is greatly appreciated.

Sincerely,

Stephen R. Colgate
Assistant Attorney General
for Administration

ATTACHMENT A

BRIEF DESCRIPTION OF PUNCH-LIST CAPABILITIES

Number	Name	Description
1	Content of subject-initiated conference calls	Capability would enable law enforcement access to content of conference calls supported by the subject's service (including the call content of parties on hold).
2	Party Hold, Join, Drop	Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference cal
3	Access to subject-initiated dialing and signaling	Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook, and other feature keys.)
4	In-band and out-of-band signaling (Notification Message)	A message would be sent to law enforcement when a subject's *service* sends a tone or other network message to the subject or associate. This can include notification that a line is ringing or bus
5	Timing to associate call data to content	Information necessary to correlate call identifyin information with the call content of a communications interception.
6	Surveillance Status Message	Message that would provide the verification that a interception is still functioning on the appropria subject.
7	Continuity Check (C-Tone)	Electronic signal that would alert law enforcement if the facility used for delivery of call content interception has failed or lost continuity.
8	Standardized delivery interface	Would limit the number of potential delivery interfaces law enforcement would need to accommoda from the industry.
9	Feature Status Message	Message would provide affirmative notification of any change in a subject's subscribed-to features.
10	Post cut-through dialing and signaling	Information would include those digits dialed by a subject after the initial call setup is completed.
11	Separated delivery	Each party to a communication would be delivered separately to law enforcement, without combining a the voices of an intercepted (conference) call.

7

The Wiretap Act of 1994

Primer for complying with the Communications Assistance for Law Enforcement Act, Public Law 103-414

Building The Wireless Future

CTIA
Cellular Telecommunications Industry Association

1 Introduction

FOR MANY YEARS, THE FEDERAL BUREAU OF INVESTIGATION sought without success to convince Congress to impose broad government-mandated technological requirements on the equipment, facilities, and services of all telecommunications carriers, including wireless systems, to facilitate law enforcement's wire and electronic surveillance capability. In support of these efforts, federal, state, and local law enforcement agencies cited the increasing number of wiretap orders directed at all users of wireless services, particularly in large metropolitan areas, and limited availability of ports on many cellular carriers' systems. In addition, the FBI sought assurances that new and advanced technologies would not inhibit lawful surveillance activities.

Finally, on October 7, 1994, after lengthy debate and intense negotiations with all segments of the communications industry the 103rd Congress completed action on H.R. 4922, the "Communications Assistance for Law Enforcement Act." The Act details a telecommunications carrier's obligation to cooperate in the interception of communications for law enforcement purposes. The act was signed by President Clinton on October 25, 1994, and became Public Law 103-414.

The law attempts to strike a balance between law enforcement needs and industry concerns. During the course of the legislative debate, Congress heard repeatedly from law enforcement, represented primarily by the FBI, that advances in digital technology and the introduction of new intelligent network services, such as call-forwarding, and Follow-Me roaming, were disabling the traditional wiretap capabilities of law enforcement. Industry representatives expressed concern over uncertainties as to liability, cost, and vague reimbursement obligations. Congress noted its concern over the potential for government mandates to dictate how private companies could research, develop, and deploy telecommunications services and products.

Up until final passage, the political agenda revolved around seemingly endless attempts to specify in legislative language the exact obligations carriers would be held to, how carrier compliance would be determined, and exactly how much and over what time period Congress would appropriate federal funds to reimburse carriers.

This primer has been prepared to provide CTIA member companies with a comprehensive analysis of the wiretap law, detailing the specific obligations imposed on carriers, manufacturers, and support service providers, along with the reimbursement procedures to be followed by both the government and the industry.

II. Industry Initiatives

A. CTIA'S FIVE-POINT WIRETAP POSITION

AT ITS MARCH 1994 MEETING, THE CTIA BOARD OF DIRECTORS ADOPTED a five-point position regarding the proposed wiretap legislation. The enacted law contains provisions addressing all five points identified by the Board:

- It includes language that makes illegal the cloning of wireless phones and the ownership of equipment to alter or modify wireless phones;
- It requires that all wireless systems shall have sufficient wiretap capacity, but that the determination of sufficient capacity will be subject to a notice and comment procedure, and recognizes that capacity demands are not uniform across all wireless markets;
- It provides that the government will reimburse carriers for the cost of upgrades necessary to achieve compliance with the Act's requirements;
- It establishes that the appropriate point in a wireless system for a legal wiretap is at the switch and that, as to roamers, wireless carriers are only required to provide information identifying the carrier within whose system a target is roaming so that a court order may be sought for a tap on the appropriate roaming switch; and
- It recognizes that no cause of action should be assessed against carriers for the failure of manufacturers or support service providers to develop software or hardware necessary to enable carriers to comply with the capability requirements of the Act.

B. TECHNICAL REQUIREMENTS AND SOLUTIONS

1. Electronic Surveillance Needs of Law Enforcement

IN JULY 1992, THE FEDERAL BUREAU OF INVESTIGATION, in cooperation with other federal, state and local law enforcement agencies, identified nine technical needs that must be met in order for law enforcement to successfully conduct court-authorized surveillance of electronic communications.[1] According to law enforcement authorities, they require:

1. Access to call content and call setup information[2] going to and from an intercept subject within a service area operated by service providers served with a court order authorizing electronic surveillance;
2. Real-time, full-time monitoring capability for intercepts;
3. Transmission of intercepted communications by service providers to remote monitoring facilities designated by law enforcement;
4. Transparency of interception-related activities to unauthorized parties, including intercept subjects, and implementation of safeguards by carriers to restrict access to intercept information;
5. Verifying information supplied by carriers which associates intercepted communications with intercept subjects, and information on services and features subscribed to by intercept subjects;
6. Increased capacity for implementing a number of simultaneous intercepts;
7. Expeditious access to the communications of intercept subjects;
8. Reliability of intercept service comparable to the reliability of service provided to intercept subjects; and
9. Quality of intercept transmissions forwarded to monitoring facilities consistent with all performance standards of the service provider.

2. Electronic Communications Service Provider Committee

IN MARCH 1993, THE ELECTRONIC COMMUNICATIONS SERVICE PROVIDER (ECSP) COMMITTEE was created by the Alliance for Telecommunications Industry Solutions (ATIS, formerly the Exchange Carrier Standards Association) in response to a request from the telecommunications industry and law enforcement that ATIS sponsor a committee to identify, and develop solutions to, technical and associated operational issues surrounding court-authorized electronic surveillance. The ECSP Committee is comprised of representatives of Regional Bell Operating Companies, interexchange carriers, wireless service providers, independent local exchange carriers, industry associations, telecommunications equipment manufacturers and law enforcement agencies. Each subcommittee of the ECSP is co-chaired by a committee member from industry and a committee member from law enforcement.

In furtherance of its mission, the ECSP Committee established a Wireless Cellular Action Team to address issues involving technical capabilities for the surveillance of electronic communications within cellular communications systems. Since its creation, this action team has examined existing cellular intercept features and evaluated the ability of these features to satisfy the needs and requirements of law enforcement for electronic surveillance. The ECSP has also created an action team focusing on the technical requirements of PCS systems.

3. Issues of Continuing Concern

CTIA CONTINUES TO WORK WITH LAW ENFORCEMENT, THE INDUSTRY, AND CONGRESS to resolve issues arising out of implementation of the new law. To that end, some carriers have expressed concern regarding the definition of "call-identifying information" which contemplates cell site or location-related information (see § 103 (a)(2)(B)), and the provision that states that a pen register order or trap and trace order may not obtain call-identifying information that discloses the physical location of the subscriber (see § 103 (a)(2)(B)). These sections may suggest that reasonable cause, the legal showing necessary to obtain a pen register or trap and trace order, is insufficient to obtain location-related information. Instead, parties may have to prove probable cause, the highest level of proof, which is necessary for an eavesdropping or search warrant.

THE ACT CONSISTS of the following three titles:

- Title I adds chapter 120 to Title 18 and is composed of twelve sections, including the wiretap capability and capacity requirements.

- Title II expands the privacy protection of the Electronic Communications Privacy Act to cover cordless telephones and certain radio-based communications; prohibits the fraudulent alteration of commercial mobile radio instruments; requires a court order for the disclosure of transactional data on electronic communications services; limits the use of pen registers that intercept information other than dialing or signalling information; and makes other technical changes.

- Title III amends the Communications Act of 1934 by requiring the FCC to prescribe rules for implementing the Act's systems security and integrity requirements, by authorizing common carriers to petition the FCC to adjust charges to recover costs of compliance, and by making certain clerical and technical amendments and eliminating expired and outdated provisions of the communications laws.

III. Relevant Section Analysis

A. Coverage and Scope, Section 102

IN 1968, CONGRESS PASSED "THE WIRETAP ACT," codified at chapter 119, 18 U.S.C. §§ 2510 - 21, as amended, that made the government's surveillance activities lawful and set up a judicial process to which law enforcement must adhere in order to obtain court-ordered wiretap authority. In response to evolving computer and telecommunications technology, the Electronic Communications Privacy Act was passed in 1986. This law amended the 1968 Wiretap Act by protecting a new class of electronic communications, including cellular telephones, paging devices, electronic mail, and computer databases. In addition, for the first time, the "technical assistance" responsibility was outlined directing telecommunications providers and other persons to furnish "all information, facilities, and technical assistance necessary" to accomplish a surveillance permitted by law.[3]

Public Law 103-414, the "Communications Assistance for Law Enforcement Act" adds, among other things, chapter 120 to Title 18, United States Code, defining in more detail the technical assistance that telecommunications carriers are required to provide in connection with court orders for wire and electronic interceptions, pen registers, and trap and trace devices. The intent is to make more certain the duty of telecommunications carriers to cooperate in the lawful interception of communications for law enforcement purposes.

Telecommunications carriers are required to have sufficient capacity to execute all electronic surveillance orders and to provide the following capabilities: (1) to expeditiously isolate the content of targeted communications transmitted within the carrier's service area; (2) to expeditiously isolate call-identifying information providing the origin and destination of targeted communications; (3) to deliver intercepted communications and call-identifying information to lines or facilities leased by law enforcement for transmission to a location away from the carrier's premises, concurrently with transmittal of the communications to or from the subscriber; and (4) to do so unobtrusively, so the targets of surveillance are not made aware of the lawful interception.

The term "telecommunications carrier" is defined, for purposes of this Act, as "any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service, as defined in section 332(d) of the Communications Act." This definition encompasses local exchange carriers, interexchange carriers, competitive access providers, wireless carriers (including cellular, PCS, and satellite providers), cable companies that offer telephony, and any other common carrier who offers wireline or wireless services for hire to the public. The definition does not cover information services, such as electronic mail providers, online services providers, or commercial Internet providers. It also does not include persons or entities engaged in providing call forwarding services, speed dialing, or the call redirection portion of a voice mail service.

In keeping with the expected increase of competitive providers of local exchange service, the FCC is authorized to designate other persons and entities as telecommunications carriers subject to the Act's assistance requirements in section 103 to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public within a state and such designation is in

the public interest. As part of its determination regarding the public interest, the Commission shall consider, among other things, whether it would promote competition, encourage the development of new technologies, and protect public safety and national security. In addition, the FCC is authorized, after consultation with the Attorney General, to exempt classes or categories of telecommunications carriers from the Act's coverage.

The scope of the assistance requirement imposed upon carriers is consistent with existing law which imposes a duty to furnish all necessary assistance pursuant to 18 U.S.C. § 2518(4). However, it is limited in several ways. First, law enforcement agencies may not dictate the specific design of systems or features, nor prohibit the adoption of any design by carriers. Further, as long as each communications message can be intercepted by at least one method, the Act leaves to the industry how to accomplish compliance. Moreover, telecommunications carriers are not required to decrypt encrypted communications that are the subject of the court-ordered wiretap, unless the carrier provided the encryption service and can decrypt the communication.

B. Mobile Service Assistance Requirement, Section 103(d)

WHEN A TARGETED SUBSCRIBER'S CALL CONTENT AND CALL-IDENTIFYING information originate outside a wireless carrier's service area, that carrier is no longer responsible for the delivery of the intercepted communications. Under such circumstances, the carrier is only responsible for notifying law enforcement as to which carrier or service provider has subsequently begun serving the target.

C. Capacity Requirements, Section 104

THE SECTION ENTITLED "NOTICE OF CAPACITY REQUIREMENTS" places upon the government the burden to estimate its capacity needs in a cost-efficient manner, while also providing carriers with a "safe harbor" for capacity. Within one year of enactment, *i.e.*, October 25, 1995, the Attorney General, after notice and comment, must publish in the Federal Register and provide to appropriate industry associations and standard-setting bodies both the maximum capacity and initial capacity required to accommodate all intercepts, pen registers, and trap and trace devices that all levels of the government expect to operate simultaneously. The maximum capacity relates to the greatest number of intercepts a particular switch must be capable of implementing simultaneously. Conversely, the initial capacity relates to the number of intercepts the government will need to operate upon the date of enforcement of this Act, *i.e.*, four years from the date of enactment.

The Attorney General is directed to develop the notices after consultation with local and state law enforcement authorities, the carriers, equipment manufacturers, and manufacturer support service providers. The Attorney General is given flexibility to determine the form of the notice; *i.e.*, the notice may be based on the type of equipment, type of service area, nature of the service area, or any other measure. The notice must identify, to the maximum extent practicable, the capacity required at specific geographic locations.

Subject to the reimbursement conditions, telecommunications carriers must ensure that, within three years after publication of the notice or four years after enactment, whichever is longer, they have the initial and

the maximum capacity to execute all surveillance orders. The Attorney General has one year, after enactment, in which to notify carriers of the government's capacity needs. If the Attorney General publishes the first capacity notice before the statutory time period of one year has elapsed, carriers must satisfy the capacity requirement by October 25, 1998, the effective implementation date of the law. However, in the event the Attorney General publishes the capacity notices after the statutory one-year deadline, carriers have three years thereafter to comply, which time period will fall after the effective date of the Act.

The Attorney General may periodically give written notice to covered entities of any necessary increases in maximum capacity. Carriers will have at least three years, and up to any additional time beyond three years as agreed to by the Attorney General, to comply with the increased maximum capacity requirements.

D. Enforcement Orders, Section 108

THE ACT PROVIDES FOR ENFORCEMENT BY THE COURTS. A court order may be issued upon the following grounds. First, the court must find that law enforcement has no reasonably achievable alternatives for implementing the order through the use of other technologies or capabilities, or by serving the order on another carrier or service provider. Essentially, the court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception.

Second, the court must find that compliance with the requirements of the Act is reasonably achievable through application of available technology, or would have been reasonably achievable if timely action had been taken. A determination of "reasonably achievable" involves a consideration of economic factors. This limitation is intended to excuse a failure to comply with the assistance capability requirements or capacity notices where the total cost of achieving compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features. In addition, this provision recognizes that, in certain circumstances, telecommunications carriers may deploy features or services even though they are not in compliance with the requirements of this Act.

In the event that either of these grounds is not met, the court may not issue an enforcement order and the carrier may proceed with the deployment, or continued offering to the public, of the equipment, facility, or service at issue.

If conditions are met for issuance of an enforcement order, the court must set a reasonable time and conditions for complying with its order. In determining what is reasonable, the court may consider, on a case-by-case basis, several enumerated factors.

The court's authority to issue enforcement orders is limited by three situations. First, an enforcement order may not be issued requiring a carrier to exceed the capacity set forth in the Attorney General's notices, issued pursuant to §104 of the Act.

Second, an enforcement order may not require a carrier to comply with the assistance capability requirements if the FCC has determined, pursuant to its authority under §109(b)(1), that such compliance is not reasonably achievable. However, if the Attorney General agrees to pay the incremental costs to make compliance reasonably achievable, pursuant to §109(b)(2), this limitation does not apply.

Finally, an enforcement order may not require a carrier to modify equipment, facilities, or services deployed before January 1, 1995, to comply with the assistance capability requirements, unless the Attorney General has agreed to pay for all reasonable costs directly associated with the modifications necessary for compliance. However, if such non-compliant equipment, facilities, or services are replaced, significantly upgraded or otherwise subjected to major modification after January 1, 1995, this limitation again does not apply.

E. Appropriations and Cost Reimbursement, Sections 109 and 110, respectively

THE ACT AUTHORIZES $500,000,000 TO BE APPROPRIATED for fiscal years 1995 through 1998 to carry out its purposes, and requires the Attorney General to pay all reasonable costs directly associated with modifications to pre-existing equipment, facilities, or services, *i.e.*, those equipment, services, or facilities deployed before January 1, 1995.

For equipment, facilities, or services that are deployed after January 1, 1995, the Act authorizes telecommunications carriers and other interested persons to petition the FCC for a determination of whether compliance with the assistance capability requirements is reasonably achievable. The FCC is given one year after the petition is filed to make its determination. In reaching its decision, the FCC is directed to determine if compliance would impose significant difficulty or expense on the carrier or users, and to consider a number of enumerated factors, including the effect on public safety and national security, the rates for basic residential telephone service, and the need to protect the privacy and security of communications not authorized to be intercepted.

If compliance with the assistance capability requirements is not reasonably achievable for equipment, facilities, and services deployed after January 1, 1995, the Attorney General is authorized, upon application by a carrier, to agree to pay additional reasonable costs to make compliance reasonably achievable. If the Attorney General elects not to pay, the equipment, feature or service in question will be considered in compliance, until it is replaced, significantly upgraded or otherwise undergoes major modifications in the ordinary course of business.

Additionally, the Attorney General is authorized, after notice and comment, to establish regulations to effectuate the timely and cost-efficient processing of any payment from the government to carriers under this Act, pursuant to chapters 119 and 120 of Title 18 of the U.S. Code, and under the Foreign Intelligence Surveillance Act of 1978. The Attorney General is further directed to consult the FCC about issuing regulations to determine reasonable costs. Such regulations must minimize the cost to the federal government and maintain the confidentiality of trade secrets, while permitting recovery from the government of (i) the direct research and development costs that have not been recovered from any other governmental or non-governmental entity, (ii) the direct costs attributable to compliance with the Act for personnel training and the deployment or installation of equipment or facilities, and (iii) in case of modifications that may be used for purposes other than for lawfully authorized electronic surveillance, only the incremental costs attributable to compliance. Such regulations will require telecommunications carriers to submit to the Attorney General claims for payment and such other information as she may require.

THE EFFECTIVE DATE FOR COMPLIANCE with the assistance capability requirements in section 103 and the systems security and integrity requirements in section 105 is set at four years after enactment, *i.e.*, October 25, 1998. All other provisions took effect upon the date of enactment, *i.e.*, October 25, 1994.

End notes:

1. The nine requirements originally identified by law enforcement in 1992 have since been reviewed by the telecommunications industry and clarified by law enforcement. They are discussed in detail in the document entitled "Law Enforcement Requirements for the Surveillance of Electronic Communications" issued in June 1994. To obtain a copy, please contact the Department of Science and Technology at CTIA.

2. "Call setup information" is the Mobile Telephone Switching Office's (MTSO's) resident internal data that is used to establish a link to the cellular subscriber. This information contains: (1) call destination (dialed digits); (2) identity of the location of the incoming call; (3) date, time, and duration of the call; and (4) first and/or last cell site used to deliver the call. "Call content information" is the content of the call (the conversation or the data transmitted during the call).

3. See, 18 U.S.C. §§ 2518(4), 3124; see also 50 U.S.C. §1802(a)(4).

PUBLIC LAW 103-414
"COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT"

TELECOMMUNICATIONS SERVICES	EFFECTIVE DATE	TECHNICAL REQUIREMENTS	COST REIMBURSEMENT	LIMITATIONS
FRAUDULENT ALTERATION OF CMRS INSTRUMENTS	Effective upon date of enactment, *i.e.*, October 25, 1994. see Title II, §206.	Offense: It is unlawful to knowingly and with intent to defraud use, produce, or traffic in, have control or custody of, or possess a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or knowingly and with intent to defraud use, produce, or traffic in, have custody or control of, or possess a scanning receiver, or hardware or software for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services. Title II, §206(a); see also Title 18, U.S.C. §1029(a) (5)-(6). Penalty: The fines pursuant to the alteration of telecommunications instruments and equipment are not more than the greater of $50,000 or twice the value obtained by the offense, or imprisonment for not more than 15 years, or both in the case of an offense involving the fraudulent alteration of a telecommunications instrument which does not occur after a conviction for another offense or an attempt to commit another offense under this subsection. Title II, §206(b); see also Title 18, U.S.C. §1029(c)(2). Definitions: The term "access device" now includes electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier. Title II, §206(c)(1); see also Title 18, U.S.C. §1029(e)(1). In addition, the term "scanning receiver" is defined as "a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119." Title II, §206(c)(4); see also Title 18, U.S.C. §1029(e)(7).	Not applicable.	Not applicable.