§ 1006(b)(3). The Department of Justice and the FBI believe that the provisions of the proposed rule impose the least financial burden on residential ratepayers consistent with the underlying need to meet the assistance capability requirements of Section 103, and industry has not indicated otherwise in prior discussions regarding the implementation of Section 103. A precise assessment of the impact of the proposed rule on residential ratepayers depends in part on cost information that is in the possession of industry rather than law enforcement. If it is shown during this rulemaking proceeding that there are alternatives to the provisions of the proposed rule that are equally effective in terms of carrying out Section 103 but would result in a smaller burden on residential ratepayers, the Department of Justice and the FBI would not object to the incorporation of such alternatives in the technical requirements and standards established by the Commission.

112. It should be noted that Section 229(e)(3) of the Communications Act of 1934 (47 U.S.C. § 229(e)(3)), as amended by CALEA, requires the Commission to convene a Federal-State Joint Board to recommend the appropriate changes to Part 36 of the Commission's rules regarding the recovery of CALEA-related costs. The Commission has initiated a rulemaking in this matter,[22] and in the course of the rulemaking, the Commission has addressed cost recovery issues for non-reimbursable CALEA expenditures and whether changes are required to Part 36 of the Commission's rules in this regard. The Commission has not yet ruled on this issue. Once the Federal-State Joint Board issues its recommendation and the Commission issues a decision in this matter, industry and

---

[22] In the Matter of Jurisdictional Separations Reform and Referral to the Federal-State Joint Board, CC Docket No. 80-286 (released October 7, 1997).

law enforcement will know more about how non-reimbursed CALEA costs are to be recovered from residential ratepayers.

113. **(d)** Section 107(b)(4). The fourth criterion in Section 107(b) is that the technical requirements and standards "serve the policy of the United States to encourage the provision of new technologies and services to the public." 47 U.S.C § 1006(b)(4). The provisions of the proposed rule are fully consistent with this criterion. The proposed rule does not impose any material restrictions on the adoption and provision of new technologies and services to the public by the telecommunications industry. It simply ensures that industry will take the steps necessary to carry out its statutory assistance obligations in conjunction with such technological advances.

114. **(e)** Section 107(b)(5). Finally, Section 107(b)(5) provides for the Commission to "provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period." The Department of Justice and the FBI suggest that the Commission provide a reasonable time for compliance with the technical standards adopted in this rulemaking proceeding by making the standards effective 18 months after the date of the Commission's decision and order in this proceeding. The Commission should further direct that industry will designate standardized delivery interface protocols within 90 days after the date of the Commission's decision and order.

B. THE COMMISSION SHOULD CONSIDER THIS MATTER ON AN EXPEDITED BASIS

115. The Commission has the authority to act on this petition on an expedited basis. Expedited consideration of a petition is warranted when a petitioning party makes a showing that it is necessary to serve the public interest. Omnipoint Corporation v. PECO Energy Company, PA 97-002, 1997 FCC LEXIS 2056, at *2 and cases cited at n.14 (Released April 18, 1997). In this case, important considerations of public safety and effective law enforcement call for expedition.

116. Expedition is warranted because effective electronic surveillance in a carrier-controlled, switch-based or network-based environment cannot be conducted without the electronic surveillance requirements set forth in this petition. This is because electronic surveillance in switch- and network-based environments depends, in great measure, upon carriers providing law enforcement the functions and capabilities that, in the past, law enforcement officers themselves could obtain. If telecommunications carriers follow only the TIA interim standard, not only will electronic surveillance information critical to criminal investigations and prosecutions be lost, but the safety of undercover officers, intercept subjects, and the public may be endangered. Thus, the deficiencies in the TIA interim standard must be remedied as soon as possible.

117. In addition, the product manufacturing and deployment schedules to produce the software and hardware necessary to comply with CALEA must be set in motion well in advance of the date that the technology actually becomes publicly available for use. If the deficiencies in the TIA interim standard are not addressed immediately, law enforcement, telecommunications carriers, and

equipment manufacturers will be uncertain as to how to proceed. Moreover, a delay in a standard that fully meets CALEA's requirements may also result in an increase in costs both to the government and to industry.

118. The CALEA-related deadlines that could be threatened by the failure to resolve the standards issue in a timely manner are set forth in the FBI's CALEA Implementation Report of January 26, 1998, which was submitted to the Chairman of the Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, House Appropriations Committee. Appendix B to that report sets forth platform roll-out dates for five switch manufacturers, all of which include software solution availability dates in the 1998-2000 time frame.[23]

---

[23] See CALEA Implementation Report, "Solution Availability Timeline," attached hereto as Appendix 6.

IV. CONCLUSION AND RELIEF REQUESTED

119. As the foregoing discussion demonstrates, the TIA interim standard omits electronic surveillance capabilities that are contemplated by the provisions and policies of CALEA, and the electronic surveillance information obtained through each capability is authorized under the applicable surveillance laws. Further, these capabilities are necessary for law enforcement properly and effectively to conduct electronic surveillance. In enacting CALEA, Congress intended to ensure that new technologies and services will not hinder law enforcement access to the communications content and call-identifying information that is the subject of an authorized electronic surveillance request. Absent the capabilities identified in this petition, the interim standard fails to carry out that intent and does not meet the requirements of Section 103 of CALEA.

120. For the foregoing reasons, the Department of Justice and the FBI, on behalf of themselves and other federal, state, and local law enforcement agencies, respectfully request that the Commission issue an order initiating an expedited rulemaking proceeding for the establishment of technical requirements and standards under Section 107(b) of CALEA. The Department of Justice and the FBI request that this petition be placed on public notice no later than Friday, April 27, 1998. Following the receipt of public comment on the petition, the Commission should issue a Notice of Proposed Rulemaking that proposes adoption of the provisions contained in this petition and proposed rule and or any other requirements and standards that the Commission determines to be appropriate under Section 107(b) and the other statutory provisions applicable to this matter.

Because of the important public safety and law enforcement interests at stake, we request that the final decision and order in this matter be issued no later than September 28, 1998.

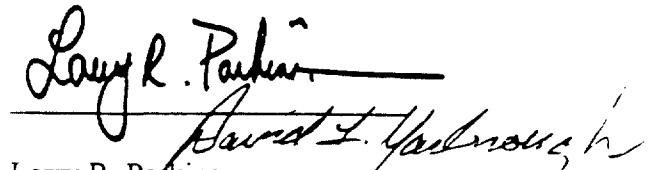
121. The Department of Justice and the FBI further respectfully request that the Commission not stay the interim standard during the consideration of the issues raised in this petition, but rather leave the interim standard in effect pending the issuance of a final decision in the rulemaking proceeding.

DATE: March 27, 1998

Respectfully submitted,

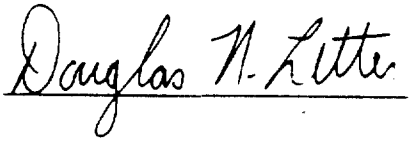
Louis J. Freeh, Director
Federal Bureau of Investigation

Honorable Janet Reno
Attorney General of the United States



Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

DAVID L. YARBROUGH
SUPERVISORY SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON DC



Stephen W. Preston
Deputy Assistant Attorney General
Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530
(202) 514-3602

Before the
Federal Communications Commission
Washington, D.C. 20554

Certificate of Service

In the Matter of:	)	
Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act	)	Docket No. _____

I, David Yarbrough, a Supervisory Special Agent in the office of the Federal Bureau of Investigation (FBI), 14800 Conference Center Drive, Suite 300, Chantilly, Virginia 20151, hereby certify that, on March 27, 1998, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of the above-referenced Joint Petition For Expedited Rulemaking, the original of which is filed herewith and upon the parties identified on the attached service list.

DATED at Chantilly, Virginia this 27th day of March, 1998.

David Yarbrough

In the Matter of
Establishment of Technical Requirements and Standards
for Telecommunications Carrier Assistance Capabilities Under the
Communications Assistance for Law Enforcement Act

Service List

*The Honorable William E. Kennard, Chairman
Federal Communications Commission
1919 M Street, N.W.-Room 814
Washington, D.C. 20554

*The Honorable Harold Furchtgott-Roth, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 802
Washington, D.C. 20554

*The Honorable Susan Ness, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 832
Washington, D.C. 20554

*The Honorable Michael Powell, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 844
Washington, D.C. 20554

*The Honorable Gloria Tristani, Commissioner
Federal Communications Commission
1919 M Street, N.W.-Room 826
Washington, D.C. 20554

*Christopher J. Wright
General Counsel
Federal Communications Commission
1919 M Street, N.W.-Room 614
Washington, D.C. 20554

*Daniel Phythyon, Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

*David Wye
Technical Advisor
Federal Communications Commission
2025 M Street, N.W.-Room 5002
Washington, D.C. 20554

*A. Richard Metzger, Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W.-Room 500B
Washington, D.C. 20554

*Geraldine Matise
Chief, Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

*Kent Nilsson
Deputy Division Chief
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 235
Washington, D.C. 20554

*David Ward
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 210N
Washington, D.C. 20554

*Marty Schwimmer
Network Services Division
Common Carrier Bureau
2000 M Street, N.W.-Room 290B
Washington, D.C. 20554

*Lawrence Petak
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

*Charles Iseman
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554 Policy Division

*Jim Burtle
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.-Room 230
Washington, D.C. 20554

Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Tom Barba
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795

Thomas Wheeler
President & CEO
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Albert Gidari
Perkins Coie
1201 Third Avenue
40th Floor
Seattle, Washington 98101

Jay Kitchen
President
Personal Communications Industry Association
500 Montgomery Street
Suite 700
Alexandria, VA 22314-1561

Roy Neel
President & CEO
United States Telephone Association
1401 H Street, N.W.
Suite 600
Washington, D.C. 20005-2164

Alliance for Telecommunication Industry Solutions
1200 G Street, N.W.
Suite 500
Washington, D.C. 20005

*International Transcription Service, Inc.
1231 20th Street, N.W.
Washington, D.C. 20036

***HAND DELIVERED**

5

Before the FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of Communications Assistance for Law Enforcement Act
Petition for Rulemaking under Sections 107 and 109
of the Communications Assistance for Law Enforcement Act
March 26, 1998

TABLE OF CONTENTS

I. Introduction -- Statement of Interest

II. Summary of Requested Relief

III. CALEA Is Not Working -- Privacy and Public Accountability Principles Are Being Ignored

IV. The Interim Industry Standard Already Goes Too Far In Enhancing Location Tracking Capabilities And Failing to Protect the Privacy of Packet Switched Communications That the Government Is Not Authorized to Intercept

A. CALEA Requires Protection of Privacy

B. By Including Location Information, the Interim Industry Standard Inappropriately Exceeded CALEA's Ceiling

C. The Interim Industry Standard Fails to Protect Privacy in Packet- Switched Networks

V. The Additional Surveillance Enhancements Sought by the FBI Have No Support to the Text or Legislative History of CALEA and Would Further Render the Standard Deficient

VI. Compliance With the Interim Standard Is Not Reasonably Achievable

VII. The Commission Has the Authority and an Obligation to Oversee CALEA Implementation

Conclusion

Footnotes

I. INTRODUCTION

The Center for Democracy and Technology respectfully petitions the Commission to intervene in the implementation of the Communications Assistance for Law Enforcement Act ("CALEA") [1], in order to protect the privacy interests of the American public, to reject attempts by the Federal Bureau of Investigation ("FBI") to use CALEA to expand government surveillance capabilities, to find compliance not "reasonably achievable" and delay compliance

indefinitely while the appropriate industry bodies develop a standard that focuses on the narrow problems that prompted Congress to enact CALEA, and to bring the surveillance redesign of the Nation's telecommunications system back under the type of public accountability that Congress intended.

The telecommunications industry and the FBI have failed to agree on a plan for preserving a narrowly-focused surveillance capability while protecting privacy. Instead, the bedrock constitutional principle of communications privacy has been shunted aside while the industry and the FBI have been mired in an argument over designing additional surveillance features into the Nation's telecommunications system.

Under unremitting pressure from the FBI, the telecommunications industry has already agreed to build surveillance features that go beyond the narrow mandate of CALEA and violate the intent of Congress. The industry in its interim standard has agreed to turn all wireless phones into location tracking devices in express contravention of the FBI Director's assurances to Congress in 1994. This capability will allow the government, on the thinnest of grounds, to follow any of the forty million Americans who use wireless phones as they go about their daily lives, from home to work to shopping to friends' houses. In addition, the standard's treatment of surveillance in packet-switched environments was premature and incomplete at best, and may result in law enforcement unnecessarily intercepting communications it is not authorized to intercept. Packet-switching forms the basis of all Internet communications, and is increasingly being used for voice communications as well. The industry standard allows the government with minimal authority to turn on a virtual spigot and get the full content of all a person's communications when the government is not authorized to intercept them, trusting to the government to sort through them and only read what it is entitled to. In an age when medical records, proprietary information, financial data and intimate thoughts are increasingly conveyed online, carriers should not provide the government with a stream of information it is not authorized to receive. CALEA requires service providers affirmatively to protect this data. These two issues alone require the Commission to exercise its authority under section 107(b) of CALEA, 47 U.S.C. ß1006(b).

Yet the FBI is pushing for additional surveillance capabilities. It is seeking to expand its wiretapping to the communications of persons suspected of no criminal wrongdoing, merely because they were on a conference call set up by a targeted suspect, who has gone on to another call. It is trying to require carriers to provide more detailed information on subscribers' communications, such as their use of long distance calling services, without meeting appropriate legal standard. It wants carriers, in disregard of the express language of CALEA, to redesign their systems to provide transactional information that is not "reasonably available." None of these add-ons finds support in the text or legislative history of CALEA, and the Commission should reject them.

The FBI's pursuit over the last three years of a 100% foolproof surveillance system -- requiring a reprogramming of the Nation's telecommunications switching systems to meet any and all contingencies identified by the FBI -- has had another consequence. The delay that has resulted while the industry developed a massive interim standard and fought with the FBI over its desired add-ons has rendered compliance with CALEA not "reasonably achievable" for equipment, facilities and services installed or deployed after January 1, 1995. CALEA section 109(b), 47 U.S.C. 1008(b). The failure of industry and law enforcement to agree on a standard occurred while the telecommunications networks were undergoing widespread change. Most systems have undergone major upgrades since January 1, 1995. Entire new technologies have been deployed. Other new systems have been developed and are about to be launched. Given the absence of an appropriate standard, it was not reasonably achievable that any of these systems be compliant with CALEA, for the simple reason that there is no agreement yet on what compliance means.

Finding compliance not reasonably achievable will require a delay in CALEA implementation.

but the real issue for the Commission is scope. In this regard, there is a convergence between the Commission's authority under section 107 to set standards and its authority under section 109 to determine if compliance is reasonably achievable. If CALEA is ever to be implemented -- if compliance is ever to be "reasonably achievable" -- the industry and the FBI will have to refocus on the narrow set of problems identified to Congress in 1994: call forwarding, speed and voice dialing, prompt access to wireless dialing information, and the effects of call waiting and conference calling on the surveillance of targeted individuals. Unless the scope of CALEA interpretation is narrowed in a way that places privacy and innovation squarely at the center of the balance -- where Congress intended them to be -- compliance will be perpetually unachievable.

This petition does not address the underlying merits of law enforcement surveillance. The FBI will undoubtedly seek to defend its conduct under CALEA by describing its view of the importance of wiretapping. Those claims are irrelevant here, for the process to date has served neither the interests of law enforcement nor of industry nor of privacy.

-- Statement of Interest

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance privacy, other civil liberties, and democratic values in the new digital media. CDT has been involved in every stage of CALEA implementation, arguing for the privacy and public accountability principles we now bring before the Commission. In July and October 1997, CDT submitted comments to the industry standards setting body on the CALEA standard, raising the location information and packet-switching objections presented here. CDT also raised those issues before the Commission in a filing last August. Last month, along with the Electronic Privacy Information Center and the Electronic Frontier Foundation, we complained to the Attorney General that the closed-door negotiations between the FBI and the industry were contrary to CALEA's privacy and public accountability principles. CALEA allows any person to file under section 107 and any "interested person" to file under section 109; CDT qualifies under both sections.

II. Summary of Requested Relief

We petition the Commission to take the following steps:

(1) institute a rulemaking under section 107(b) and determine that the location tracking and packet switching provisions in the interim industry standard violate CALEA and render the standard deficient;

(2) examine the privacy implications of surveillance in a packet-switching environment and, specifically, the technical requirements for separating call-identifying information from call content, so law enforcement does not receive communications it is not authorized to intercept, and develop an appropriate standard under section 107(b);

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

(4) use the section 107(b) authority to remand development of a CALEA standard to the appropriate industry bodies, directing them to narrow the interim standard to focus on the specific problems of call forwarding, speed and voice dialing, prompt access to wireless dialing information, and the effects of call waiting and conference calling on the surveillance of targeted individuals, or undertake to pare back the standard itself to the same end; and

(5) under section 109(b), find compliance with the assistance capability requirements not

reasonably achievable for equipment, facilities and services installed or deployed after January 1, 1995, and indefinitely delay implementation of the statute, while industry develops a narrowly focused standard, for only after the scope of CALEA's mandate is properly construed to be narrow can the Commission set appropriate implementation dates.

III.CALEA Is Not Working -- Privacy and Public Accountability Principles Are Being Ignored

It is abundantly clear that CALEA is not working. It is not working because the FBI was years late in publishing its surveillance capacity notice and has now issued a notice that still fails to provide the specificity and certainty required by the statute and that still imposes on carriers vastly exaggerated requirements. [2] It is not working because industry and the FBI decided not to focus on the limited number of problems brought to Congress' attention in 1994, but rather undertook to develop a comprehensive standard, which the FBI then defeated as a national standard. When industry went forward and adopted an interim standard, the FBI cast a cloud of uncertainty over it and continued to push for expanded capabilities. CALEA is not working because, as the FBI admitted privately to the Commission staff some time ago and has now admitted to Congress, compliance technology will not be available to meet the October 1998 deadline. [3] It is not working because nearly four-fifths of the funds for compliance have not been appropriated, while the costs of retrofitting have increased dramatically. And it is not working because the Justice Department and the industry have taken the redesign of the Nation's telecommunications system for surveillance purposes behind closed-doors in a process not subject to the public accountability that Congress wanted.

The debate about CALEA is not only about cost or about how much to extend the compliance and "grandfather" deadlines, although those are issues that will require Commission consideration. Fundamentally, the debate is about who controls the Nation's telecommunications system, about what values guide its development, and about how decisions are made about its design.

Under CALEA, Congress decided that the Nation's telecommunications carriers should control the design of the telephone system through publicly available standards, subject not to the dictates of law enforcement but rather to oversight by this Commission and the courts.

Congress intended that development of the telecommunications system should be guided by a balance among three factors: preserving a narrowly-focused law enforcement surveillance capability, protecting privacy, and promoting innovation and competitiveness within the telecommunications industry. H.Rept. 103-827, p. 9-10.

And finally, Congress decided that decisions about implementing CALEA were to be made through publicly accountable procedures that allowed for participation of public interest organizations.

All three of these principles have been violated. It is time for the Commission to restore them.

IV. THE INTERIM INDUSTRY STANDARD ALREADY GOES TOO FAR IN ENHANCING LOCATION TRACKING CAPABILITIES AND FAILING TO PROTECT THE PRIVACY OF PACKET SWITCHED COMMUNICATIONS THAT THE GOVERNMENT IS NOT AUTHORIZED TO INTERCEPT

Congress intended that the capability assistance requirements of CALEA would serve as "both a floor and a ceiling" on government surveillance demands. H. Rept. 103-827, p. 22. The interim industry standard is deficient because, under pressure from the FBI, the industry agreed that wireless telephone companies would turn their customers' phones into location tracking devices, contrary to the intent of Congress.

Furthermore, in a decision that has potentially far-reaching implications for the future of telephony, the Internet and government surveillance, the interim standard would allow telecommunications companies using "packet switching" to provide the full content of customer communications to the government even when the government is only authorized to intercept addressing or dialing data. Thereby, the standard fails to satisfy the privacy protections of the wiretap laws and fails to meet CALEA's requirement to "protect the privacy and security of communications ... not authorized to be intercepted." CALEA section 103(a)(4), 47 U.S.C. 1002(a)(4).

A.CALEA Requires Protection of Privacy

CALEA imposes on the telecommunications industry four requirements. Three of these requirements are intended to preserve law enforcement's surveillance capabilities, but the fourth also mandates protection of privacy. Carriers are required to ensure that their systems are capable of (1) expeditiously isolating and enabling law enforcement to intercept call content; (2) expeditiously isolating and enabling the government to access reasonably available "call-identifying information," a defined term; (3) delivering intercepted communications and call-identifying information to the government in a format that allows them to be transmitted to a law enforcement listening plant; and (4) doing so "in a manner that protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted" and the confidentiality of the interception. CALEA section 103(a)(1) - (4), 47 U.S.C. 1002(a)(1) -(4) (emphasis added).

Section 103(a)(4) imposes on telecommunications carriers for the first time ever an affirmative obligation to protect the privacy of communications and call-identifying data not authorized to be intercepted. This has direct implications for the packet-switching issue.

Moreover, because Congress was concerned with a blurring of the distinction between call-identifying data and call content, it included in CALEA an amendment to the pen register statute to require law enforcement when executing a pen register to use equipment "that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." CALEA section 207(b), codified at 18 U.S.C. 3121(c). (The wiretap laws set a much higher standard for government access to call content than to dialing information, allowing access to the latter upon a mere assertion of relevance to an ongoing investigation.) These provisions mean that carriers have an obligation to withhold from law enforcement the content of communications when the government has only pen register authority to intercept dialing or addressing information. They also show that Congress meant to limit call-identifying information to mean "dialing and signaling information utilized in call processing," placing most of the "punchlist" items outside the scope of CALEA.

B.By Including Location Information, the Interim Industry Standard Inappropriately Exceeded CALEA's Ceiling

The interim industry standard requires cellular and PCS carriers to provide law enforcement agencies with location information at the beginning and end of any cellular and PCS communication. It was the express intent of Congress, supported by the Director of

the FBI on the record in public testimony, that CALEA not include any requirement to provide

location or tracking information. [4]

At the joint House and Senate hearings leading to enactment of CALEA, FBI Director Freeh expressly testified that CALEA would not require carriers to make location information uniformly available. Director Freeh testified that "call setup information" (later changed to "call-identifying information") as a CALEA requirement was not intended to include location information. Director Freeh was very clear in disavowing any interest in covering such information:

> "[Call setup information] does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called åtracking' information."

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103rd Cong. 6 (1994).

Despite these assurances, the FBI pressured the standards organization to include tracking information. Industry acceded to the FBI and put location information in the interim standard on the ground that location information was already available in many wireless systems. But the addition of location information is not a simple give away with no practical consequences. Putting location information in the standard means that manufacturers will design it in as a permanent and ubiquitous feature of their switches. And it sets a precedent for future FBI demands to expand the definition of call-identifying information in this and other contexts.

Adding location information violated Congress' intent that the capability assistance requirements of CALEA would serve as "both a floor and a ceiling" for government surveillance capabilities. H. Rept. 103-827, p. 22. Congress "expect[ed] industry, law enforcement and the FCC to narrowly interpret the requirements." Id. at p. 23. This goes to the core of the balanced approach Congress intended in CALEA. The statute was intended to create a process for preserving a narrowly-focused surveillance capability. It was not intended to afford the FBI leverage to steadily increase its capabilities. Changes in technology will bring ebbs and flows in government surveillance capability. The statute was not intended as a ratchet device to standardize every increase in the surveillance potential of telecommunications technology. By adding location information, carriers standardized a capability that Congress had specifically intended to exclude, violating Congress' ceiling principle.

C.The Interim Industry Standard Fails to Protect Privacy in Packet-Switched Networks

In the future, telecommunications systems will rely increasingly on "packet switching" protocols similar to those used on the Internet. This development has potentially profound implications for government surveillance. In a packet switching system, communications are broken up into individual packets, each of which contains addressing information that gets the packets to their intended destination, where they are reassembled. Previously utilized primarily on the Internet for electronic communications, this technology offers substantial advantages in the voice environment as well, and telecommunications companies are beginning to incorporate it in their systems.

On the apparently untested assumption that it is not feasible to provide signaling information separate from content in a packet switching environment, industry's interim standard allows companies to deliver the entire packet data stream -- including the content of communications -- when law enforcement is entitled to receive only dialing or signaling information under a so-

called pen register order. Such orders are issued without probable cause and without the discretionary review accorded to full call content interceptions. The proposed CALEA standard relies on law enforcement to sort out the addressing information from the content, keeping the former but ignoring the latter. This violates section 103(a)(4)(A) of CALEA, which requires carriers to ensure that their systems "protect[]the privacy and security of communications and call-identifying data not authorized to be intercepted."

CDT highlighted this issue in its ballot comments on the proposed industry standard. The draft was modified but it still allows carriers to provide all packets to the government, relying on the government to sort out the addressing information from the content. This approach, were it followed, could totally obliterate the distinction between call content and signaling information that was a core assumption of the Electronic Communications Privacy Act and of CALEA itself. In the old analog systems, law enforcement agencies authorized to receive dialing information were provided with access to the target's entire line, including content. With subsequent developments in technology, dialing information for call-routing purposes was carried on a channel separate from the call content. In this respect, technology itself enhanced privacy, creating an environment in which a law enforcement agency conducting a pen register would receive only so much as it was entitled to receive, and no more. Absent CALEA, packet switching might have undone that privacy enhancement, for both addressing and content travel together in packet-switched systems. But CALEA imposed on the telecommunications industry an affirmative obligation to protect communications not authorized to be intercepted. CALEA, section 103(a)(4). In a packet-switched environment, this means that carriers must separate addressing information from content (subject to CALEA's overall reasonably achievable standard). The interim industry standard has failed to require this. Instead, industry and FBI have tacitly agreed not to try to ensure that law enforcement agencies get only the information appropriate to the level of authorization in hand.

V. THE ADDITIONAL SURVEILLANCE ENHANCEMENTS SOUGHT BY THE FBI HAVE NO SUPPORT IN THE TEXT OR LEGISLATIVE HISTORY OF CALEA AND WOULD FURTHER RENDER THE STANDARD DEFICIENT

At least in the foregoing respects, and perhaps in others, the interim standard already exceeds the outer limits of what Congress intended to mandate through CALEA. The FBI, however, has made it clear that it is not satisfied with the standard. The FBI has urged expansion of the standard to require functionality that goes even further beyond anything Congress contemplated. If the FBI's demands were accepted, the standard would be rendered further non-compliant with section 103(a)(4) and compliance would become even less reasonably achievable.

There is no support in the language of CALEA or the legislative history for the FBI's claim that a CALEA standard must include the additional surveillance features on the FBI's "punch-list." There is no evidence that Congress intended to mandate these specific additional capabilities. Since it is clear that Congress intended to defer to industry, and since there is no evidence that Congress intended to mandate the specific features sought by the FBI, neither the industry nor the Commission has authority to adopt a standard that adds additional provisions sought by the FBI.

The following "punch-list" items are of specific concern:

(1) Multi-party monitoring -- At the time CALEA was enacted, the FBI expressed concern that 3-way calling features interferred with its ability to listen to the communications of a target. Now, however, based on an overly-expansive reading of both the electronic surveillance laws

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]